Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework

D7.1 Project Management strategy project handbook

Document Identification			
Status	Final	**Due Date**	15/12/2017
Version	1.34	**Submission Date**	30/11/2017

Related WP	**WP7**	**Document Reference**	D7.1
Related Deliverable(s)	None	**Dissemination Level (*)**	PU
Lead Participant	ATOS	**Lead Author**	Rosana Valle Soriano Jose Francisco Ruiz
Contributors	------	**Reviewers**	Samuel Fricker (FHNW)
			Sotiris Ioannidis (FORTH)
			George Oikonomou (CITRIX)

This document is issued within the frame and for the purpose of the SMESEC project. This project has received funding from the European Union's Horizon2020 Framework Programme H2020-DS-SC7-2016 under Grant Agreement No. 740787 and supported by Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document Information

List of Contributors	
Name	Partner
Rosana Valle Soriano	ATOS
Jose Francisco Ruiz	ATOS

Document History			
Version	Date	Change editors	Changes
0.1	09/10/2017	ATOS	First draft, TOC.
0.2	12/10/2017	ATOS	Section 3 and Executive Summary.
0.3	18/10/2017	ATOS	Section 1
0.4	23/10/2017	ATOS	Section 2.1, section 2.2
0.5	24/10/2017	ATOS	Section 2.3.
0.6	30/10/2017	ATOS	Section 3
0.7	08/11/2017	ATOS	Revision from PC
0.8	15/11/2017	ATOS	Final refinements
0.9	16/11/2017	ATOS	Ready for review
1.0	20/11/2017	ATOS	Review comments applied (FORTH)
1.1	22/11/2017	ATOS	Review comments applied (FFHNW)
1.2	23/11/2017	ATOS	Changes in section4 (risk management process)
1.3	24/11/2017	ATOS	CITRIX comments and changes applied.
1.31	30/11/2017	ATOS	Risk section modifications and small refinements in references section.
1.32	05/12/2017	ATOS	Review of PC
1.33	05/12/2017	ATOS	Review comments applied (FORTH)
1.34	15/12/2017	ATOS	Quality review and submission to EC.

Table of Contents

Document Information 2
Table of Contents 3
List of Tables 5
List of Figures 6
List of Acronyms 7
Disclaimer 8
Executive Summary 9
1 Introduction 10
1.1 Project Identification 10
1.2 Project Summary 10
1.3 Work plan 11
1.4 Work Package List 11
1.5 Milestones 12
1.6 Project Representatives 13
1.6.1 EC Representative 13
1.6.2 Consortium representatives 13
2 Project Management 14
2.1 Project Organization 14
2.2 Communication 18
2.2.1 Contact List 18
2.2.2 Emails and Distribution Lists 18
2.2.3 Communication tools 19
2.2.4 Document Management 20
2.2.5 Security measures 22
2.3 Quality Assurance 22
2.3.1 Document Identification 23
2.3.2 Documents format and templates 23
2.3.3 Deliverable review quality process 25
2.3.4 Deliverable Roles 26

2.3.5 Deliverable review process 27
2.3.6 Schedule 28
2.3.7 List of deliverables 29
2.4 Project Meetings 30
2.4.1 Project Review meetings 31
2.5 Project Reporting 31
2.5.1 Semestral Activity Report 31
2.5.2 Official Reporting (EC) 32
2.5.3 Periodic Reports 32
2.5.4 Final Report 33
2.5.5 Summary of periodic reporting and schedule 33
3 Dissemination, Communication and Collaboration Activities 35
3.1 Procedure 35
3.2 Rules for publications 36
3.3 Travelling to non-EU countries 36
4 Risk Management 37
4.1 Risk Management Process 37
4.1.1 Plan Risk Management 38
4.2 Identify Risks 43
4.3 Risk Analysis 43
4.4 Plan Risk responses 43
4.5 Control Risks 44
4.6 Common Risk Management Errors 45
5 Conclusions 46
References 47
Annex I 48

List of Tables

Table 1: Project identification 10
Table 2: List of WPs 11
Table 3: List of milestones 12
Table 4: List of consortium representatives 13
Table 5: List of consortium representatives with specific roles 15
Table 6: List of PMB representatives 16
Table 7: List of Advisory Board Members 17
Table 8: List of Strategic Management Committee Members 17
Table 9: Document writing 28
Table 10: Peer Review Process 28
Table 11: Review Approval 28
Table 12: Quality Review 28
Table 13: Review process Timeline 29
Table 14: Project meetings 31
Table 15: Semestral Activity Report 32
Table 16: Summary of Project Reporting 33
Table 17: Risks Management RASCI Chart 38
Table 18: Scale of Probability 39
Table 19: Impact on Schedule 40
Table 20: Impact on results 40
Table 21: SMESEC Risk Register Fields 41
Table 22: SMESEC Risk Register File 42

List of Figures

Figure 1: Project governance structure ____ *15*
Figure 2: Screenshot of OwnCloud interface for the first log in ____ *21*
Figure 3: Folders structure in SMESEC OwnCloud repository ____ *22*
Figure 4: Process of production of deliverables: stages and document state ____ *27*
Figure 5: Reporting Schedule ____ *34*
Figure 6: Risk Management Process Cycle ____ *37*
Figure 7: SMESEC's Gantt Chart ____ *48*

List of Acronyms

Abbreviation / acronym	Description
AB	Advisory Board
CA	Consortium Agreement
CO	Confidential
DB	Directory Board
DoA	Description of Action
Dx.y	Deliverable Number
EC	European Commission
EU	European Union
GA	Grant Agreement
IMC	Innovation Management Committee
MS	Milestone
PC	Project Coordinator
PO	Project Officer
PU	Public
PMB	Project Management Board
RP	Reporting Period
RASCI	Responsible, Approve, Support, Consult, Inform
SC	Security Committee
SMC	Strategic Management Committee
SME	Small and Medium Enterprise
STMC	Scientific and Technological Management Committee
TL	Task Leader
WP	Work Package
WPL	Work Package Leader

Disclaimer

The content of this document is based on the management, quality and risk assessment methodology defined by the Project & Proposals Management unit of Atos Research & Innovation for research projects and proposals. This methodology is the a common ground for all projects and proposals where ATOS participates as project coordinator and/or acts as quality manager, though the methodology is adapted to the particularities of each project. This methodology is intended as a general reference to support ATOS coordinators to perform their role in a professional and harmonized manner in all projects where ATOS plays such a role. Finally, the methodology also relies on a set of templates, documents and guidelines that are also adapted to each project.

Executive Summary

This document is the overall Project Management Plan for the SMESEC project. It defines the common management procedures to be used during the project, the organization and time-scales of the activities to perform. It is the main contribution to T7.1 – Project coordination including operational management to be monitored during the lifetime of the project.

This Project Management Plan describes the processes that will be used during the project. It may also qualify the way in which these processes are applied and define project-specific information such as responsibilities. In particular, the following topics are described in this deliverable:

- The quality requirements of the communication procedures.
- The specific quality requirements regarding storage, backup and archiving.
- The quality standards of deliverables and their acceptance criteria.
- The quality procedures to be applied by project management.
- The specific quality requirements of deliverable documents and software items.
- The risks management along the project lifetime.

1 Introduction

1.1 Project Identification

Project acronym	SMESEC
Project title	Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework
Project type	IA
Call	H2020-DS-SC7-2016
Topic	DS-02-2016 Cyber Security for SMEs, local public administration and Individuals
Contract	740787
Project start date	01/06/2017
Estimated end date	31/05/2019
Estimated total time	36 months

Table 1: Project identification

1.2 Project Summary

SMESEC is a European project funded by the Horizon 2020 programme of the European Commission and the Swiss State Secretariat for Education, Research and Innovation (SERI) whose aim is to support SMEs in managing network information security risks and threats, as well as in identifying opportunities for implementing secure innovative technology in the digital market. The project will develop a cost-effective framework composed of specific cyber-security tool-kit, which assesses SMEs state-of-the-art services and products and decreases cyber-security threats to protect European citizens and businesses.

The SMESEC solution will be deployed and validated in four different and transversal use cases:

(1) e-Voting, which presents one of the most critical environments of the project from the security point of view related to electoral processes
(2) Smart City with the SenseCity platform (http://sense.city) that provides the tools that activate citizen's creativity, imagination and communication, engages urban thinking and improves the relationship between citizens, the city municipality and city's public services
(3) Industrial IoT: Worldsensing Industrial solutions aim to detect and prevent possible risks to structures and infrastructures by monitoring their operations and status in real time, and finally
(4) Smart Grids: The PowerVAS™ platform enables electric energy utility companies in Europe and around the world to deploy digital value added services for their customers.

Additionally SMESEC will organize an open call during the final year of the project that will allow SMESEC to validate the proposed solution across more SMEs belonging to different areas. This open call will allow SMESEC to collect additional evaluation results and make the necessary adjustments towards a robust and flexible security framework capable of supporting companies and organizations with limited budget.

1.3 Work plan

The following section describes the development procedure to be followed during the project as defined in the "Description of Action" (DoA) [2] of the contract.

The work in the SMESEC project is organized in seven work packages, briefly described below:

- **WP1**: Ensures compliance with the ethics requirements.
- **WP2**: Analyses specific SMEs security requirements, clearly assessing weak points and current limitations. Additionally, creates a security awareness enhancement roadmap for SME.
- **WP3:** Designs and develops the SMESEC Framework solution and implements the security awareness and training roadmap.
- **WP4:** Integrates the SMESEC security framework in the four SME pilot scenarios proposed in the project for validation.
- **WP5**: Final adjustments toward a close-to-market solution running on real operational scenarios; as well as organizes and executes the SMESEC open call.
- **WP6:** Starts from the very beginning, capturing and collecting all project contributions for communication, exploitation, and standardization purposes.
- **WP7**: Deals with overall project management aspects.

In case of discrepancy please refer to the last version of the DoA approved by the consortium and PO. The time schedule planned for the project is presented in Annex I

1.4 Work Package List

WP Number	WP Title	Lead Beneficiary	Person Months	Start Month	End Month
WP1	Ethics requirements	ATOS	N/A	1	36
WP2	Adaptation of SMESEC security components to SMEs requirements	CITRIX	84	1	6
WP3	SMESEC security framework development for small-medium companies and organizations	IBM	242,5	1	36
WP4	Integration of SMESEC security framework to e-Voting, Smart City, Industrial Services and Smart Grids pilots	ATOS	109	10	24
WP5	Refinement, Evaluation, Demonstration and Security Assessment of the SMESEC platform in operational environment (TRL8/9)	WoS	121	19	36
WP6	Exploitation, dissemination and standardization activities	EGM	72	1	36
WP7	Project Management	ATOS	45	1	36
		TOTAL	**673,5**		

Table 2: List of WPs

1.5 Milestones

Milestone Number	Milestone title	WP	Lead beneficiary	Due Date (in months)	Means of verification
MS1	Security analysis and preliminary information	WP2	CITRIX	6	D2.1, D2.2, D2.3
MS2	Architecture system design	WP3	IBM	9	D3.1
MS3	First release: preliminary version of the SMESEC security Framework	WP3	IBM	18	D3.2, D3.4
MS4	Security awareness and training – I	WP3	EGM	18	D3.5
MS5	Prototype ready for operational tests	WP3	IBM	24	D3.3, SW release I
MS6	Final SMESEC security framework	WP3	CITRIX	36	D3.7, SW release – FINAL
MS7	Security awareness and training – II	WP3	EGM	36	D3.6
MS8	Preliminary pilots integration report	WP4	ATOS	18	D4.1, D4.3, D4.5, D4.7
MS9	Final pilots integration report	WP4	ATOS	24	D4.2, D4.4, D4.6, D4.8, D4.9
MS10	Trials settings and configuration	WP5	GRIDP	24	D5.1
MS11	System ready for experimentation	WP5	SCY	27	D5.2
MS12	Prototype demonstration successfully conducted	WP5	WoS	32	D5.3
MS13	Final SMESEC security framework (TRL 8) evaluation results	WP5	FORTH	36	D5.4, D5.5
MS14	The exploitation and dissemination plan is ready	WP6	EGM	6	D6.1
MS15	The business model for exploitation is ready	WP6	ATOS	34	D6.5
MS16	Final project quality demonstration: exploitation, dissemination and standardization report	WP6	EGM	36	D6.2, D6.3, D6.4
MS17	Project management strategy	WP7	ATOS	6	D7.1
MS18	Project report: First, Second and Third year	WP7	ATOS	36	D7.2, D7.3, D7.4

Table 3: List of milestones

1.6 Project Representatives

1.6.1 EC Representative

A Project Officer (PO) in the EC is the person in charge of evaluating, monitoring and negotiating the SMESEC project, performing the financial evaluation of the project and providing support to the project management body. The Project Officer of SMESEC is:

Name: **Georgios Kaiafas**

E-mail georgios.kaiafas@ec.europa.eu

1.6.2 Consortium representatives

The SMESEC consortium is composed of **12 partners**. The key contact person from each organization is cited in the table below:

No	Acronym	Partner	Country	Contact person	email
1	ATOS	ATOS SPAIN SA	SP	Jose Francisco Ruiz	jose.ruizr@atos.net
2	WOS	WORLDSENSING	SP	Francisco Hernandez	fhernandez@worldsensing.com
3	UOP	UNIVERSITY OF PATRAS	GR	Kostas Lampropoulos	klamprop@ece.upatras.gr
4	FORTH	FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	GR	Sotiris Ioannidis	sotiris@ics.forth.gr
5	EGM	EASY GLOBAL MARKET SAS	FR	Philippe Cousin	philippe.cousin@eglobalmark.com
6	SCY	SCYTL SECURE ELECTRONIC VOTING S.A	ES	Adria Rodríguez-Pérez	adria.rodriguez@scytl.com
7	GRID	GRIDPOCKET	FR	Filip Gluszak	filip.gluszak@gridpocket.com
8	FHNW	FACHHOCHSCHULE NORDWESTSCHWEIZ	CH	Samuel Fricker	samuel.fricker@fhnw.ch
9	CITRIX	Citrix Greece MEPE	GR	Yannis Bournakas	yannis.bournakas@citrix.com
10	IBM	IBM ISRAEL SCIENCE & TECHNOLOGY LTD	IL	Sharon Keidar	sharon@il.ibm.com
11	BD	BITDEFENDER SRL	RO	Ciprian Oprisa	coprisa@bitdefender.com.
12	UU	UNIVERSITY OF UTRECHT	NL	Marco Spruit	marco@spru.it

Table 4: List of consortium representatives

2 Project Management

This section presents the project general management structure, and cooperation procedures to follow along the lifetime of the project.

The bodies and structures are the ones described in the DoA. We present them here in order to facilitate the understanding of the government bodies. In case of updates the valid (and more actual) organization would be the one described in the last version of the DoA.

2.1 Project Organization

The project management structure is based on the following roles:

Project Coordinator (PC): Responsible for the general/administrative management of the project, including:

- Coordinating and controlling the major activities of the project and supervising the progress of the project.
- Defining and reviewing the scientific and technical strategy of the project, and driving the implementation of the project according to that strategy.
- Acting as an intermediary between the consortium and the EU Commission. It is also responsible for ensuring that both financial and contractual obligations are met.
- Managing all the communications to/from the EU Commission, the periodic reporting, and organizing the review meetings with the Project Officer.
- Collecting all partners' financial statements and audit certificates, and reporting the periodic financial summaries and resource efforts spent by each partner.
- Managing the granted EU contribution and distribution of funds among the SMESEC partners according with the actual allocated efforts.

Work package Leader (WPL): Each WPL is appointed by the partner responsible for the work package, and has the responsibility to coordinate and monitor the work performed within the WP. The main responsibilities are listed below:

- Planning and monitoring of the WP activities, and ensuring the communication among the participants of the WP.
- Organizing the production and internal review of the work package deliverables and assessing the progress of the work package on a regular basis.
- Responsible of the coordination, interaction and collaboration with other WPs, and to facilitate the communication between different WPs.

Task Leader (TL): Each Task Leader is appointed by the partner leading a task, as defined in each work package. TLs coordinate the work of the task among the task participants. TLs are coordinated by the respective WPLs for their work package.

The table below represents the partners appointed for the SMESEC management structure.

ROLE	PARTNER	RESPONSIBLES
Project Coordinator	ATOS	Jose Ruiz
Technical Manager	CITRIX	George Tsolis
Innovation Manager	WoS	Francisco Hernández
Strategy Management Committe	EGM	Philippe Cousin
Security Committee	CITRIX	George Oikonomou
WP1 Leader	ATOS	Jose Ruiz
WP2 Leader	CITRIX	George Oiknomou
WP3 Leader	IBM	Sharon Keidar
WP4 Leader	ATOS	Jose Ruiz
WP5 Leader	WoS	Francisco Hernández
WP6 Leader	EGM	Philippe Cousin
WP7 Leader	ATOS	Jose Ruiz

Table 5: List of consortium representatives with specific roles

The roles presented in Table 5function under the supervision and management of the following project bodies, as it is described in the figure below (Figure 1).

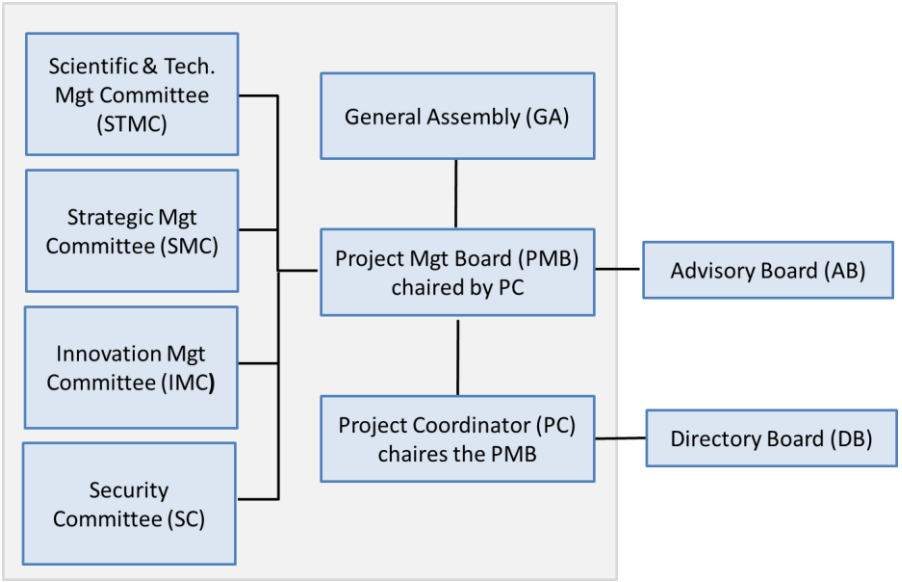

Figure 1: Project governance structure

General Assembly (GA): It is the main decision making body of the project, chaired by the PC and consists of one representative from each partner in the Consortium. The GA provides a common forum for discussion between the partners for defining, monitoring, reviewing and evaluating the overall progress of the project. The GA is also responsible for discussing administrative and strategic management issues of the project, and issues related to standardization, dissemination and exploitation activities.

Project Management Board (PMB): The PMB is chaired by the PC and consist of one representative of each partner. The Project Management Board is a working committee of the General Assembly. Among its responsibilities is to define the direction and strategies of the project, to actively control the overall success of the project and to support the PC in the strategic management of the project, ensuring thereby that all partners can meet their individual responsibilities.

PARTNER	RESPONSIBLE
ATOS	Jose Ruiz
FORTH	Sotiris Ioannidis
IBM	Sharon Keidar
FHNW	Samuel Fricker
Utrecht University	Marco Spruit
EGM	Philippe Cousin
CITRIX	George Oiknomou
University of Patras	Kostas Lampropoulos
Gridpocket	Filip Gluszak
Scytl	Adria Rodríguez-Pérez
Wos	Francisco Hernandez
Bitdefender	Ciprian Oprisa

Table 6: List of PMB representatives

Directory Board (DB): The DB is chaired by the PC and composed by several experts from ATOS to provide support to the PC. The SMESEC project will benefit from the experience of the DB members, not only on issues related to project management, but also on outreach activities through ATOS's network of contacts.

Advisory Board (AB): The Advisory Board consists of a panel of external experts from research, academia and the industry. These experts will not be involved in the day-to-day project work, but they will be in permanent contact with market related trends and evolution, and thus, they can significantly contribute to the project by providing their knowledge, recommendations and feedback. The AB will evaluate the project's technical progress and will provide the necessary feedback in order to ensure that evolution of the project is in the direction to fulfil its objectives and goals. Tentative members for the AB are listed below, it is important to highlight that this list might suffer slightly changes according to the needed expertise necessary for the project when the meetings of the advisory board are done.

EXPERTS	COMPANY	CONTACT PARTNER
Dr. Ioannis Askoxylakis	Hellenic Authority for Communication Security and Privacy	FORTH
Prof. Dr. Ir. B. Preneel	KU Leuven	FORTH
Dr. Abbas Shahim	chair of the IFIP's Working Group WG 11.5 on IT Assurance and Audit	UU
Dr. Omar Elloumi	oneM2M TP chair, Nokia Bell Labs and CTO	EGM
Dr Petros Ganos	Municipality of Patras	UoP

Table 7: List of Advisory Board Members

Strategic Management Committee (SMC): Led by the WP6 Leader, responsible for the strategic evolution of the project through a continuous monitoring of the different project activities to guarantee alignment with external project efforts and initiatives. Also, the SMC will monitor the information security landscape for identifying impactful emerging information security threats, and it will take the required actions to ensure that the project meets the emerging security needs.

NAME	ORGANIZATION
Philippe Cousin	EGM
Samuel Fricker	FHNW
Alberto Miranda	ATOS
Marco Spruit	UU

Table 8: List of Strategic Management Committee Members

Scientific and Technological Management Committee (STMC): Is led by the WP2 leader and consists of the Project Coordinator and all Work Package Leaders. It is responsible for the implementation of the direction and strategies of the project, as defined by the Project Management Board (PMB). Specifically, the STMC is responsible for the overall technical development of the project, the synergetic communication between the different activities and the coordination of the work packages, by ensuring that WP technical dependencies are managed properly. This committee is also responsible for the day-to-day management and monitoring of the research and technical activities of the project.

Innovation Management Committee (IMC): It is led by the WP5 Leader and includes members from other, mainly industrial, partners. It is responsible for all activities related to project innovation. This committee is responsible for keeping under systematic review the current market trends, products and solutions. It will also provide directions to increase the impact of the project, and additionally, it will monitor the outcomes of the technical process of SMESEC in order to identify business opportunities.

Security Committee (SC): The SC is responsible of reviewing all information handled and produced by SMESEC (particularly the project deliverables) and deciding if they disclose sensitive information, and/or if they are suitable for dissemination in the public domain. They will also indicate whether the

information has to be filtered out before publishing or if the concerned deliverable has to be upgraded from Public (PU) to Confidential (CO) (if it discloses confidential information of a partner).

2.2 Communication

2.2.1 Contact List

We have prepared and make available to the consortium a document that compiles the project participant names, their email addresses, their work phone numbers, their Skype IDs and the SMESEC mailing lists.

The latest updated version of the contact list can be found in the project repository in OwnCloud:

https://repository.atosresearch.eu/owncloud/index.php/apps/files/ajax/download.php?dir=%2FSMESEC%2FCommunication%20and%20partners&files=Partners%20SMESEC_v021.xlsx

For details to access the repository, please refer to section 2.2.4.

2.2.2 Emails and Distribution Lists

Several mailing lists have been created in order to collaborate and exchange information among the partners. These lists are

- **SMESEC**: for general purposes related to the project
  smesec@lists.atosresearch.eu
- **SMESEC-WP1**: for those partners working in Ethical aspects of the project (WP1).
  smesec-wp1@lists.atosresearch.eu
- **SMESEC-WP2:** for those partners working in SMESEC WP2
  smesec-wp2@lists.atosresearch.eu
- **SMESEC-WP3**: for those partners working in SMESEC WP3
  smesec-wp3@lists.atosresearch.eu
- **SMESEC-WP4**: for those partners working in SMESEC WP4
  smesec-wp4@lists.atosresearch.eu
- **SMESEC-WP5:** for those partners working in SMESEC WP5
  smesec-wp5@lists.atosresearch.eu
- **SMESEC-WP6**: for those partners working in SMESEC WP6
  smesec-wp6@lists.atosresearch.eu
- **SMESEC-MGMT**: For administrative, legal and financial issues. The right place to be aware about cost statements, EC payments, signature of relevant documents, and other management aspects (WP7).

  smesec-mgmt@lists.atosresearch.eu

These lists are moderated and hosted by ATOS, the project coordinator. They keep a history of the most relevant emails along the project. The amount and subjects for the lists are dynamic. Unused lists will be removed and additional lists can be created under request.

For adding new members to any of the above mentioned mailing list you can contact the PC.

2.2.2.1 General rules:

In order to avoid an excess of mailing traffic and foster a rational use of lists, some rules have been recommended:

- Address information ONLY to involved parties in communication: do not systematically put everyone in copy.
- Use preferably the official mailing lists to address a team.
- Use explicit subject title for each email. The subject should always start with [SMESEC] followed by a clear indication of the content.
- Change the subject title of the mail if you are changing the topic of the e-mail.
- If you have to attach a file, try to ZIP files to compress 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 in the OwnCloud document repository and just inform the relevant people of the location of the file.
- Keep your questions and comments relevant to the focus of the discussion group.
- Keep paragraphs and messages short and to the point.
- If you should find yourself in a disagreement with one person, make your responses to each other via mail rather than continue to send messages to the list or the group. If you are debating a point on which the group might have some interest, you may summarize for them later.
- When posting a question to the discussion group, request that responses be directed to you personally. Post a summary or answer to your question to the group.
- When sending a message to more than one mailing list, especially if the lists are closely related, apologize for cross posting.
- When replying to a message posted to a discussion group, check the address to be certain it's going to the intended location (person or group). It can be not useful if they reply incorrectly and post a personal message to the entire discussion group that was intended for an individual.

For details to access the repository, please refer to section 2.2.4.

2.2.3 Communication tools

Several communication tools will be used along the project:

- **Phone calls:** these will be used preferably between only two partners, and will be especially useful for short conversations or clarifications.
- **Teleconferences**: these will be preferred when several partners need to clarify or discuss the progress of the project or any other issues as well as for periodical checkpoints to keep all partners updated, such as the monthly PMB telcos. The tools to use are:
    - Preferably a web-based communication tool called **Circuit.**
    - Alternatively on Lync.
    - Alternatively on Skype.

These web-based tools allow adding conference arrangements to be added to the MS Exchange calendar, and allow sharing screens, files and chat.

- **PMB telcos**: periodic project follow-up calls will be performed within the project lifetime. The basic rules to follow are:
    - At project-level, a **monthly** conference call will be carried out the first **Thursday** of each month at **14:00 pm** CET. In case of public holiday, or any other critical reason for not being able to have the meeting with a minimum number of partners (WPL and PC), the PC will provide to the consortium with a new date chosen by all partners.
    - 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).
    - WP calls advisable at request of project members.
    - The organization setting up the call is in charge of providing the conferencing infrastructure. If no infrastructure is available, the PC will provide it (Circuit).
    - Brief agenda at least a couple of days before the call.
    - Minutes kept by the organizer.
    - Specific conference calls and meetings are expected to be organised when preparing deliverables or other intermediate milestones.
- **GitLab**

In addition to the OwnCloud project repository, which is the official document store of the project and where all final versions of official deliverables must be kept, ATOS has set up a GitLab platform to support SMESEC technical work. The GitLab platform [6] offers a Git repository for code versioning, reviews, issue tracking and wikis, among other features.

In principle, the GitLab platform is intended to be used as follows:

- in the context of WP3 to support integration of the tools and development of the SMESEC Framework
- For WP4, to support refinement and integration of the SMESEC Framework in the pilots
- in the context of WP5 , to support development activities, testing and integration

The GitLab platform is managed by ATOS and can be accessed upon request to the PC. The default access is restricted to members of the consortium, but it is possible to define publicly accessible git projects to support dissemination of project results to a wider community.

2.2.4 Document Management

A document repository in OwnCloud has been set up for the SMESEC project, offering an internal tool for collaboration inside the Consortium. Documents such as final deliverables, working version of the deliverables, agenda, minutes, presentations, dissemination material, among others, will be stored by the respective partners within the repository. This OwnCloud repository is hosted by ATOS, the project coordinator.

Access to the OwnCloud repository

Consortium members can access the SMESEC repository through this link:

https://repository.atosresearch.eu/owncloud/index.php/apps/files/?dir=%2FSMESEC

Consortium members receive a password that allows them to access the repository, read and save documents and create folders. Each user has its own user ID and password. Account information and

new accounts are provided by the ATOS team. Access to the repository can be requested by email to the PC. You will need to send your name, last name, institution and email address.

Figure 2: Screenshot of OwnCloud interface for the first log in

SMESEC Repository

The project repository has the following folders:

- **Administrative Data:** This is the place where the legal documents of the project – Grant Agreement (GA) [3], Consortium Agreement (CA) [1], annexes to be filled and project amendments.
- **Communication & Partners**: This folder contains the contact list of the consortium.
- **Final version of deliverables**: In this folder the final version of the deliverables are stored in PDF and Word format.
- **Meeting & Telcos**: This folder contains the information, agenda presentations, and pictures and minutes of each meeting that is being celebrated in the project, either face to face meetings or telco meetings.
- **Project Boards:** This folder will include the members of each project board such as advisory board members, PMB members, strategy board members, etc.
- **Project Risks:** This folder will contain a file with all risks encountered along the project lifetime.
- **Templates:** This folder contains all the templates of the project (deliverables, peer review deliverables, minutes, agenda, presentations, etc.)
- **WP1…WP7:** These folders contain working documents for each WP. At least the final version of each deliverable in doc format has to be uploaded to its folder.

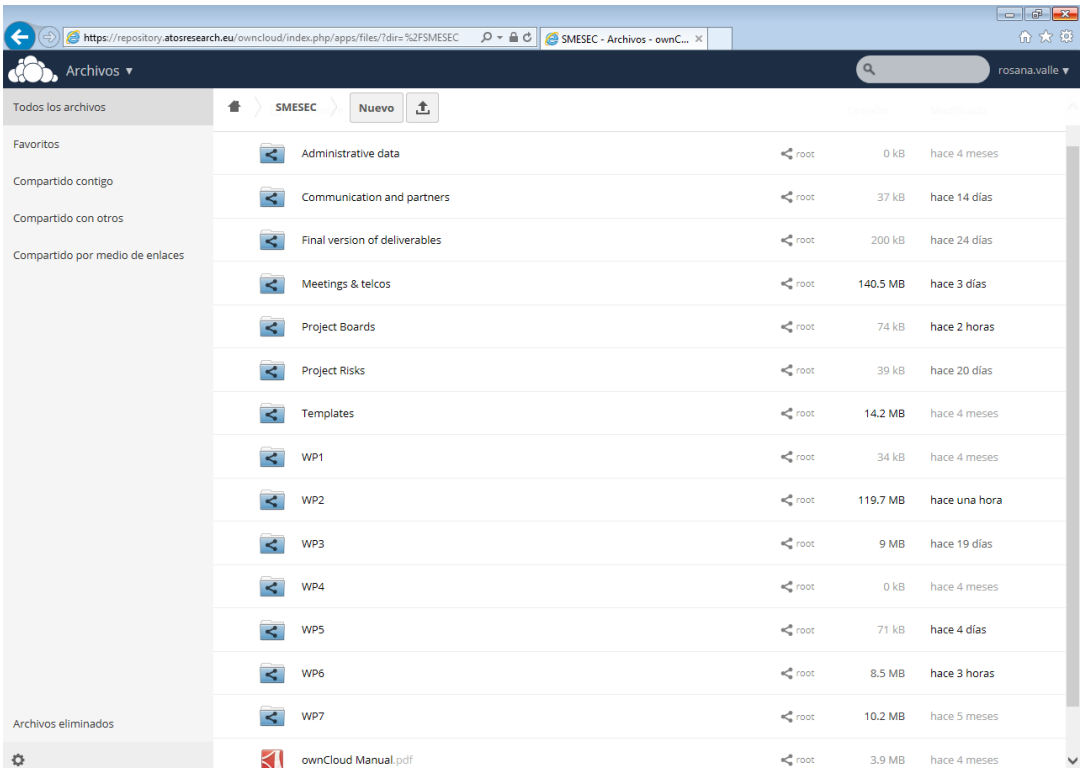

Figure 3: Folders structure in SMESEC OwnCloud repository

2.2.5 Security measures

According to the DoA (section 3.2.3), the project will establish appropriate policies and rules for the management of background and foreground Intellectual Property Rights (IPR) for the knowledge developed within the SMESEC Project.

The Consortium Agreement has already established rules for the use of foreground, side ground and background knowledge and its distribution within the project as well as rules for handling sensitive or confidential information, as well as the terms of intellectual properties management for the project.

The CA has also included an initial collection of a list of reusable and non-reusable pre-existing know-how (background knowledge) available at the start of the project, and new know-how (foreground knowledge) generated by the R&D activities during the project.

Regarding dissemination activities, the procedures for validating results and knowledge in the project are defined in D6.1 section 4.5.

2.3 Quality Assurance

In SMESEC one of the main outcomes are the deliverables. They are mainly reports (documents) and demonstrators (software). This section describes how to assure quality in the delivery of the project outcomes.

2.3.1 Document Identification

Project deliverables for the European Commission serve as the outcome of the project progress. They consist of a combination of documents such as written reports as well as prototype software releases. The European Commission requires that all non-document deliverables be documented appropriately as a written report.

Before being uploaded to the Owncloud repository and delivered to the EC, all the deliverables must be named following this format:

SMESEC_DX.X_Complete_title_of_the_deliverable _vX.X.pdf.

(Project name + deliverable number+ deliverable title + version, all separated by underscore instead of spaces)

2.3.2 Documents format and templates

The following sections presents the standard tools that will be used for the generation of project documents.

Word processor and programs

The standard word processor for documents production is **Microsoft Word (docx)**. For the documents that may need modifications and contributions from several partners, the "Track Changes" function shall be enabled and used.

The standard tool to make presentations is **Microsoft PowerPoint (pptx)**.

Final deliverables will be available also in **PDF** format.

Templates

All documents must use the corresponding templates, available at the repository under the "Templates" folder as mentioned before and produced by the ATOS team. These templates define specific styles for normal text and titles, tables, figures, etc.

All project templates are already available at the repository under the "Templates" folder:

https://repository.atosresearch.eu/owncloud/index.php/apps/files?dir=/SMESEC/Templates

There are templates available for the following purposes:

- Deliverable;
- Deliverable peer review;
- Presentations;
- Agenda;
- Minute;
- Reporting: QARs, PPRs, Financial.

About fonts and format

The following points that shall be taken into account when producing a document:

- The set out font of the document **Times New Roman (font 11)** and the given template for creating all documents is available for all partners.

- The text format within tables and figures will depend on the format and size of the table or figure.
- It is strongly recommended not to use titles further than level 3.

Reference

- All references will be included in the references section at the end of the document; the references must be simple with a sequential reference number.
- References must be created by means of cross-reference:

  - First, create your section of References at the end of the document. Follow the example below.

    [1] **Books:** Author Surname, First name initials, (Year of Publication), *Book Title (Edition),* Publisher, City of Publication. (Example: Levenstein, H. A. (2003), *Revolution at the table: The transformation of the American diet*, University of California Press, Berkeley.)

    [2] **Articles in Journals:** Author Surname, First name initials, (Year of Publication), *Article Title, Periodical, Volume and Issue, Pages.* (Example: Hoxby, C. M. (2002), The power of peers, *Education Next*, *2*(2), 57-63.)

    [3] **Articles on Websites:** Author Surname, First name initials, (Year of Publication or most recent Update), *Website/Article Title, Website URL,* [Date of access yyyy-mm-dd]. (Example: Cain, A., & Burris, M. (1999). *Investigation of the use of mobile phones while driving*, http://www.cutr.eng.usf.edu/its/mobile_phone_text.htm, retrieved 2017-11-06)

    [4] **Deliverable:** [PROJECT NAME] [*DELIVERABLE TITLE*] [LEAD AUTHOR (surname,name)] [et al. if needed] [YEAR]. (Example: WITDOM. *D2.2 - Functional analysis and use cases identification*. Alberti Francesco et al., 2015)

    [5] **Websites:** [WEB NAME], [*PAGE TITLE*],[URL], [retrieved date yyyy-mm.dd] (Example: SMESEC. *Deliverables*. http://www.smesec.eu/deliverables , retrieved 2017-11-06)

  - Place your cursor where the **cross-reference** should be inserted
  - Add any introductory text and brackets ([ ]) required.
  - Click **References | Cross-reference**. A Cross-reference dialog box will appear.
  - Click on the drop down menu **Reference** type and select "Numbered item"
  - Click on the drop down the **Insert reference** to and select "Paragraph number"
  - Available headings, captions, footnotes in your document will have appeared in the list of the dialog box. It you have created the section of references as explained the first step of this list; you will find your bibliographic references at the end. Select the item you wish to reference.
  - Click **Insert.**

Figures and tables

When figures are included in the document, an index of figures shall be included at the beginning of the document. The same shall be done in case of tables.

Lists and bullets

Bullets will use, at the first level, a black dot. The text in the bullet shall end with a point if it is composed of complete phrases as in the present bullet, or without any ending if it is composed of a list of items as in the bulleted list in next section.

Length and style

The advisable length of the document for all SMESEC deliverables is as necessary for describing in a concise and clear way all the objectives and results planned for that deliverable (bearing in mind the tasks that contribute to it).

We encourage all partners to keep the document short and simple. The value of a document cannot be measured by its length, but by its valuable content.

All leaders of deliverables will follow the next suggestions for making easy-to-read all deliverables:

- **Avoid repeating content**. Shorter documents and shorter sentences tend to have more impact.
- When referring to a long name, **write out the full name only once**. Explain the meaning of acronyms in a table at the beginning of the document.
- **Avoid repeating the executive summary**, the introduction and the purpose of the document sections. These sections tend to be the same repetition over and over and this should be avoided.

    - Executive Summary is a one/two page/s presentation of the content of the document. The reader may read only this page and understand how we have reached our conclusions.
    - Introduction establishes briefly the objectives of the document, the context and describes the structure of the document.

Annexes

All additional information not relevant for the work being done, but related, shall go into the Annexes. The Annexes sections will include the additional information to the main body of the document that is not essential for the understanding of the document, but it is complementary.

2.3.3 Deliverable review quality process

The intention of the deliverable review and quality process is to ensure that the document has been reviewed by a broad spectrum of individuals against a set of criteria. In order to submit to the EC only documents of the highest quality level possible, once a deliverable is finished, it will go through a two-stage review process, plus a quality check. **Three different people** (**1 peer reviewer, 1 approval, 1 quality manager**) within the consortium will review the document before uploading it to the EC platform.

The list of appointed reviewers for each document is available in the Owncloud repository.

https://repository.atosresearch.eu/owncloud/index.php/apps/files/ajax/download.php?dir=%2FSMESEC&files=SMESEC%20DELIVERABLE%20LIST%20v3.xlsx

There are two artefacts that support the successful operation of this process:

- ***Template for Deliverable*:** ensures a homogeneous structure and visual aspect for all deliverables.
- ***Template for Peer Deliverable Review:*** used to report on the results of the review process and to communicate deliverable editors' comments, questions, clarifications and proposals for changes in the deliverable.

The last version of both documents is available in the project repository, in a dedicated folder for templates already mentioned in section 2.3.2.

Interim versions of the deliverable as well as deliverable review reports must be kept in the project repository, in the corresponding deliverable folder, to make them available to the consortium.

2.3.4 Deliverable Roles

Deliverable Leaders refers to a member of the SMESEC project who is responsible for the writing/main author of the deliverable. The author must comply with the following rules:

- The author will provide a ToC (Table of Contents) and must indicate there which contributions are expected from other partners.
- The owner (author) should compose the documents on the official SMESEC template and respect all the indications provided in the previous sections.
- The ultimate responsibility for the quality of deliverables resides on the author, although each contributor engaged is responsible for its actual production.
- The author will propose the deliverable schedule in accordance with the delivery dates and milestones specified in this project - including deadlines. It will be a requirement to provide deliverables for review by the "reviewers" at **least 2 weeks before submission to the EC**. This deadline will be enforced in order to ensure all deliverables have a reasonable amount of time for review and updating and ensure the best quality of the document.

Deliverable contributor: participates in the production of the deliverable by contributing with content and supporting the leader in producing a high quality deliverable, addressing reviewers' comments and requests.

Peer reviewer: refers to a member of the consortium that is responsible for the revision of the internal review of the deliverable (before sending it to the EC). The reviewer must not be a direct contributor to the deliverable and is responsible for carefully reviewing the content of the deliverable, ensuring the deliverable objectives are met, from a scientific/technical point of view, but also that the overall review objectives are fulfilled by the deliverable.

The peer reviewer must fill in the review report, using the template created for that purpose, available in the link below:

https://repository.atosresearch.eu/owncloud/index.php/apps/files?dir=/SMESEC/Templates/Deliverable%20Peer%20review%20Report

Comments can be also provided in the document using MS Word features such as track-changes or review comments. The peer reviewer must upload the deliverable document (with comments) and the review report to the project repository, and notify the deliverable leader accordingly.

Approval Reviewer: The approval process consists in ensuring that the comments/requests in the peer review report have been indeed addressed by the deliverable leader/contributors, keeping in touch with the peer reviewer if necessary. The appointed approver must update the corresponding section in the review report, in due time. Optionally, the approver can make other suggestions or comments to the deliverable leader. The deliverable document and the updated review report must be uploaded to the project repository and notify the deliverable leader accordingly.

Deliverable Quality Manager: a member of the coordination team (ATOS) will perform a last round of proof-reading, to find and correct typographical errors and mistakes in grammar, style, spelling and layout that the modifications done when addressing review comments and requests may have introduced. It is responsible for uploading the final version of the deliverable to the correct location in the project repository and into the European Commission platform.

2.3.5 Deliverable review process

The review process of a deliverable is presented in the figure below, where all different stages of production of status of the deliverable are provided. The figure also indicates, for each stage (in rounded rectangle), the corresponding document state (in a rectangle).

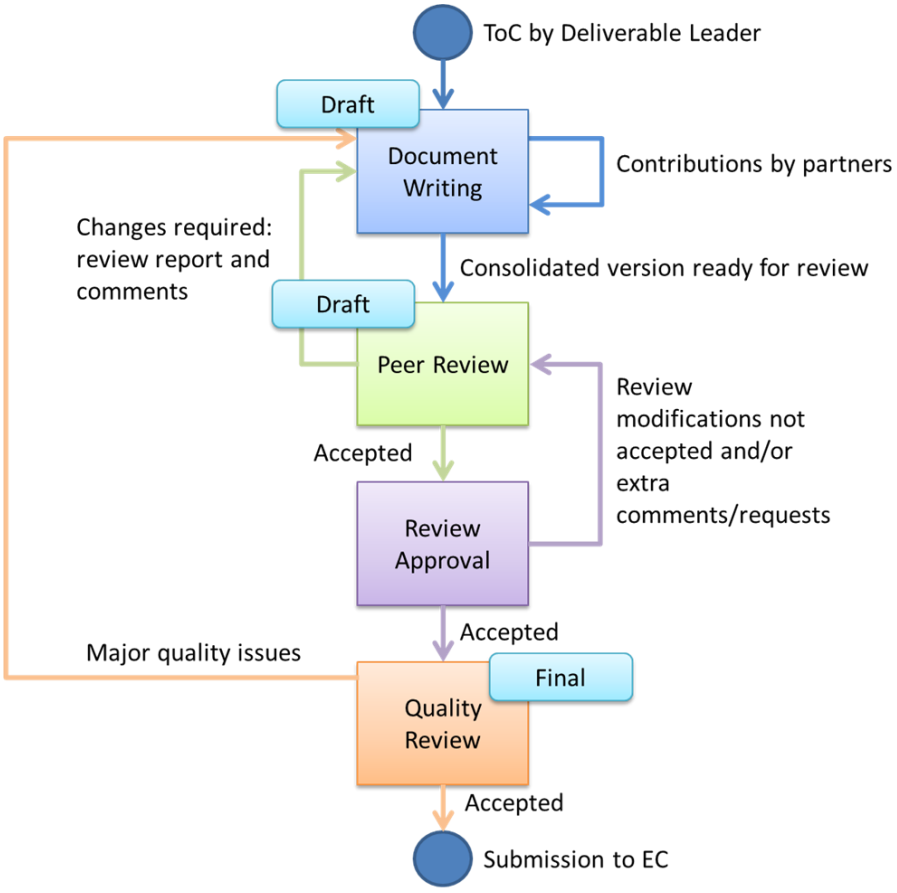

Figure 4: Process of production of deliverables: stages and document state

All different stages are fully explained in the tables below:

Process Stage	**Document Writing**
Responsible role	Deliverable Leader
Other roles involved	Deliverable contributors
Deliverable state	Draft

Input	N/A
Output	Deliverable document

Table 9: Document writing

Process Stage	**Peer Review**
Responsible role	Appointed Peer Reviewer
Other roles involved	Deliverable Leader
Deliverable state	Draft
Input	Deliverable document: consolidated draft, ready for review
Output	Deliverable Review Report Deliverable document with comments (optional)

Table 10: Peer Review Process

Process Stage	**Review approval**
Responsible role	Appointed Approval Reviewer
Other roles involved	Deliverable Leader
Deliverable state	Draft
Input	Deliverable document: updated addressing peer review comments and requests for changes Deliverable Review Report
Output	Deliverable Review Report: updated with approval reviewer comments Deliverable document with comments (optional)

Table 11: Review Approval

Process Stage	**Quality Review**
Responsible role	Quality Manager (ATOS)
Other roles involved	Deliverable Leader
Deliverable state	Final
Input	Deliverable document: approved
Output	Deliverable document: final, ready for submission to EC

Table 12: Quality Review

2.3.6 Schedule

The entire review process may require about four weeks which allows various feedback loops between the different reviewers and the deliverable leader (and contributors). The schedule proposed in the next table is recommended and deliverable leaders are encouraged to adhere to it. However, the timing of specific review stages can be reduced if previously agreed between the deliverable leader and the corresponding reviewers.

Review Process Stage	Starts When	Duration	Roles involved
Peer Review	4 weeks before submission date	2 weeks	Deliverable Leader Peer Reviewer
Approval	2 weeks before submission date	1 week	Deliverable Leader Approval Reviewer Peer Reviewer (optional)
Quality Check	1 week before submission date	1 week	Deliverable Leader Quality Manager

Table 13: Review process Timeline

It is the responsibility of the deliverable leader to make sure the document is ready for starting peer review process by the corresponding date and therefore, to plan the previous writing phase (and interim draft versions) accordingly.

2.3.7 List of deliverables

The most updated list of deliverables including the reviewers (peers and approvals) for each deliverable can be found in Owncloud:

https://repository.atosresearch.eu/owncloud/index.php/apps/files/ajax/download.php?dir=%2FSMESEC&files=SMESEC%20DELIVERABLE%20LIST%20v2.xlsx

The appointment of a reviewer to a particular deliverable will follow some basic rules in each case:

- **Peer reviewer**

  The person appointed must have a special interest in the topic covered by the deliverable (e.g. a related WP/task/deliverable leader, main role in a task that depends on the work described in the deliverable).

- **Approval reviewer**

  The person appointed must not be a direct contributor to the document under review, although someone else belonging to the same organisation could have been involved in the writing. Ideally, should be a senior role.

In the appointment of reviewers, it should be taken into account the overall workload to avoid an unbalanced assignment among consortium partners. The list of appointed reviewers can be updated whenever it is considered necessary, but any request for a change in the list must be communicated to the Coordinator and validated by the Consortium.

2.4 Project Meetings

In order to ensure maximum profitability from project meetings, the following actions will be carried out by the PC for each meeting. These actions involve all Consortium members:

- **Initial announcement of the meeting**, with proposal of tentative dates and venue. A consultation round (doodle polls - www.doodle.com) among all participants is done and the, according to the availability, the final dates and venue will be set.
- 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 and some facilities for sharing documents, presentations, etc.
- **Submission of a draft agenda for the meeting**. All participants will be able to contribute to the final agenda with remarks and additions to the draft.
- **Submission of the final agenda for the meeting**, incorporating the suggestions made by all the participants. The agenda will be stored in the OwnCloud repository.
- **Submission of draft minutes** for the meeting. All participants will be able to contribute to the final minutes with remarks and additions to the distributed draft.
- **Submission of the final minutes** for the meeting, incorporating the suggestions made by all the participants. The minutes will be stored in the Owcloud repository.
- **Phone conferences** are always the preferred means over face-to-face meetings, in order to minimize travelling within the project.

The main meetings within this project are classified in the table below:

Name	Description	Periodicity
GA Meetings	The GA is the main decision making body of the project. The participation is mandatory. If a voting is necessary it is allowed only one vote per partner.	Approximately every six months
PMB meetings	The PBM meetings could be either phone calls or face to face meetings. Face-to-face meetings will be co-located, as much as possible, with General Assembly meetings to avoid unnecessary travelling.	– Monthly conference calls. Second Thursday of each month at 14:00 CET – Approximately every six months (face to face meetings)
STMC meetings	The Project Coordinator will organize regular STMC meetings between all WPLs to monitor the scientific and technical activities	– Telco meetings – Approximately every six months (face to face meetings)
WP or Task specific workshops (face-to-face)	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 2 month**s in advance. The PC will consult the PMB to evaluate possibilities of co-location together with other WP/Task meetings or to allocate it within an already scheduled GA	– Phone conferences or face to face meetings on demand

	meeting close in time.	
Review meetings	According to the Grant Agreement, the consortium will also meet for an annual EC review. Before this review, a general meeting will be held for the preparation of the topics that will be presented in the review. The participation of at least one person per partner is also requested.	– M12 – M24 – M36

Table 14: Project meetings

2.4.1 Project Review meetings

As established in the Grant Agreement, there are three review meetings where the EC representative and the external reviewers appointed by the Project Officer will evaluate the project execution and progress towards the objectives declared in the DoA.

As we have mentioned in the Table 14, the three meetings have been scheduled for M12, M24, and M36.

The PC (with the support of the WPL and all consortium members) will organise and prepare the review meetings in advance, following the guidelines listed next:

- Using and providing **templates for review** presentations available in the project repository;
- Preparing **the agenda for review** preparation and for the review meeting;
- **Presiding overall 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 Manager.

2.5 Project Reporting

In order to keep track of the use of the technical achievements , the status and progress of the project, the usage of budget and efforts, there are reports that will be submitted internally and to the EC periodically as indicated by the contract. These are described in the present section.

2.5.1 Semestral Activity Report

Partners must report their activities in each WP and Task where they are involved, every 6 months. This Semestral Activity Reports (SARs) will help WP and Task leaders monitor the progress of the work towards achieving specific objectives, but also track partner contributions in order to detect potential deviations from the plan early enough to implement mitigation actions. The template is available in the SMESEC repository in Owncloud:

https://repository.atosresearch.eu/owncloud/index.php/apps/files?dir=/SMESEC/Templates/Interim%20report%20template

The table below summarizes the most important points about the Semestral Activity Report:

Frequency	Every 6 months (CA)	
Responsible	PC – WP leaders	
Level of detail	WP - Task	
Content	- Activities carried out by beneficiaries in each task - Dissemination, exploitation activities - Progress towards objectives - Milestones achieved, deliverables submitted - Costs (estimates) - Deviations from work-plan in effort and costs, mitigation actions - Risks foreseen and encountered along the period by WP	
Procedure	Beneficiary	- Describe work done in each Task-WP - List dissemination, exploitation activities - Provide estimate effort and costs, justify deviations
	WP Leader	- Collect input from partners - Complete WP-level Information - Approve partners' report

Table 15: Semestral Activity Report

2.5.2 Official Reporting (EC)

The EC established 2 reporting periods in the Grant Agreement:

- **RP1: from month 1 to month 12.**
- **RP2: from month 13 to month 36.**

These reports entail each partner's declaration of financial statements costs and efforts (real) for the period.

2.5.3 Periodic Reports

The Project Management Reports are contractual reports that will be submitted to EC every 12 months. According to the DoA, they are depicted in deliverables:

- **D7.2 at M12 (aligned to RP1).**
- **D7.3 at M24.**
- **D7.4 at M36 (final, aligned to both RP2 and Final Review).**

The structure and content of the periodic reports is defined by the Grant Agreement and can be summarized as follows:

Periodic technical report containing:

- An explanation of the work carried out by the beneficiaries overview of the progress towards the objectives of the action, including milestones and deliverables, differences between work expected and carried out, exploitation and dissemination of the results.
- A summary for publication by the EC, answers to the H2020 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)

Periodic financial report containing

- Individual financial statement from each beneficiary.
- Explanation of the use of resources, subcontracting and in-kind contributions provided by third parties from each beneficiary.
- ATOS, as coordination party, will be in charge of collecting from all consortium partners the information required to fill in the Periodic Reports.

2.5.4 Final Report

A final report has to be submitted within 60 days after the end of the project. This final report shall comprise:

- A final **publishable summary** report covering results, their exploitation and dissemination, conclusions and socio-economic impact of the project.
- A 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** are required when the accumulated funding surpasses 325.000€.

2.5.5 Summary of periodic reporting and schedule

This section summarizes all the expected reports along the project in terms of responsibilities, periodicity and a brief description, as well as the reporting schedule foreseen along the project life time.

Report	Content	Responsible	Distribution	Periodicity
Semestral Activity Report (SAR)	Project activity, estimated costs and effort from all partners.	WPL, partners and project coordinator	Only Consortium	Every 6 months
D7.2, D7.3 and D7.4 Project Management Report	Overview of Project, activity and WP progress. Includes actual costs and effort of all partners. Financial Statements + Audit Certificate if required (325,000€ accumulated requested funding)	WP leaders, Technical Coordinator and Project Coordinator	EC	Every 12 months
Final Report	Published summary and financial report summary	WP leaders, Technical Coordinator and Project Coordinator	EC	60 days after the end of the project

Table 16: Summary of Project Reporting

The reporting schedule is summarized in the figure below:

European Commission

Reporting Period No.	From Month	To Month	Duration
1	June 2017	November 2018	18
2	December 2018	May 2020	18

Coordinator - ATOS

Rep. No.	Type	From Month	To Month	Duration
1	Interim	June 2017	November 2017	6
1	Interim	December 2017	May 2018	6
1	**P1**	**June 2017**	**November 2018**	**18**
2	Interim	December 2018	May 2019	6
2	Interim	June 2019	November 2019	6
2	**P2 - Final**	**December 2018**	**May 2020**	**18**

Figure 5: Reporting Schedule

3 Dissemination, Communication and Collaboration Activities

In line with the official project dissemination and communication strategy, the members of the consortium will attend meetings to present regularly project advances and results.

3.1 Procedure

Any dissemination, communication or collaboration activity planned by consortium members should be in line with the dissemination and communication strategies defined in deliverable D6.1 Dissemination Plan and Market Analysis,

A **spreadsheet** for announcing and reporting these activities (both planned and already executed) is available in the project repository under WP6 folder. All partners must keep it up to date with their own activities.

The procedure for validation of publications and communications is described below:

1. Any partner that plans to do a publication, presentation or talk to outside the project consortium should communicate the proposal to the WP6 Leader and the PC by email, at least **1 week** before the actual publication deadline. The following details should be provided:
   - Title and a summary/abstract of the content to be disclosed.
   - In which format the information will be disclosed (paper, journal, presentation given, poster, press release, talk in an event, etc.)
   - Point to the dissemination and communication activities spreadsheet in the repository for further details of the proposal on the venue, etc.
2. The WP6 Leader and PC **will have 3 working days** for objecting.
3. If nothing is objected within this timeframe the proposal will be considered approved.
4. If there is any objection, the author will be requested to provide more details or questioned separately for a more in-depth review of the proposal. An amendment of the content of the publication could be requested too.
5. The entire process should not take more than **7 working days**. If no agreement can be reach within 7 days, the Project Coordinator should call for a PMB extraordinary meeting to discuss the matter as per stated in the Consortium Agreement (section 8.3 Dissemination).

3.2 Rules for publications

Rules for publications are available in D6.1 section 4.5.4.

Official logos of the project for publication can be found in the project repository:

https://repository.atosresearch.eu/owncloud/index.php/apps/files?dir=/SMESEC/Templates/Logo

3.3 Travelling to non-EU countries

Should you plan to attend a dissemination event in a non-EU country and to claim the associated travel costs to the EC in the corresponding financial statement, it must be notified in advance to the PC for validation with the PO.

Since the validation by the PO could take some time (and more details/clarifications about the trip could be required), it is advised that project partners communicate the PC about the details of the planned trip well in advance, to avoid purchasing flights, hotels, conference registration, etc. in vain.

The following rules apply in this case:

- The following information should be provided by email to the PC about the planned trip to non-EU countries, which will be forwarded to the P.O.:
  - Destination country/city.
  - Trip dates.
  - Purpose of the trip (provide as much details as possible to justify the trip: e.g. conference name, link, reason for attendance, title/abstract of the paper/presentation, etc.)
  - Relation with SMESEC.
- The PC will try to speed up the process as much as possible, but it is the responsibility of project partners to decide when is exactly "well in advance".
- Costs that do not have the specific mail with the OK from PC will not be accepted in cost claims.

4 Risk Management

The risk management process is vital for any project in order to anticipate situations that can affect the normal progress or even put in danger the continuation of the project. This anticipation will provide the SMESEC consortium with enough information to take decisions accordingly and act beforehand to minimise the impact of the risks identified.

The Risk Management methodology presented in this guide follows the PMI (Project Management Institute) guidelines as presented in the PMBOK® Guide [[5]].

4.1 Risk Management Process

Risk management will be implemented in SMESEC through five processes, in a continuous improvement approach during the project lifetime:

- Plan Risk Management.
- Identify Risks.
- Risk Analysis.
- Plan Risk Responses.
- Control Risks.

Figure 6: Risk Management Process Cycle

4.1.1 Plan Risk Management

As depicted in the figure above, the first process to take place is the **Plan Risk Management**.

At this stage, all the following processes needed for the proper risk management process of the project are designed. Also, risks categories, roles and their responsibilities, definition of probability/impact of the risks are defined in order for the processes of "Identify Risks" and "Risk Analysis" to take place.

4.1.1.1 Risk Categories:

In order to identify properly the risks of the project, the following categories of risks are defined at this stage of the project. Any new category identified through the course of the project will be part of the risk management process.

These are the risk categories identified at this stage of the project SMESEC:

- Financial risks
- Communications
- Scope
- Cost
- Resources
- Technical

4.1.1.2 Roles and responsibilities

The Project Coordinator will lead and supervise the risk management activities in coordination with the PMB

Other roles involved during the risk management processes with a major responsibility are: Technical Coordinator, and Work Package Leaders.

The next Risk Assessment Matrix (RAM) summarises the roles and responsibilities within the project, according to a RASCI model: The RASCI model [4] describes the participation of various roles in completing tasks or deliverables for a project or business process.

RASCI CHART	ROLES				
	PC	TC	WPL	TL	PARTNER
Plan Risk Management	R	C	C	C	S
Identify Risks	A	C	R	C	S
Risk Analysis	A	C	R	C	S
Plan Risk responses	A	C	R	C	S
Control Risks	A	C	R	C	S

Table 17: Risks Management RASCI Chart

- **Responsible (R)** is the entity(s) who is the owner of the problem, generally the entity that does the work
- **Accountable (A)** is the entity to whom "R" is accountable and the authority who approves to sign-off on work, there is max 1 entity accountable per task/process
- **Supportive (S)** is the entity(s) that provides resources or has a supporting role
- **Consulted (C)** is the entity(s) that provide information and/or the necessary expertise to complete the task
- **Informed (I)** is the entity(s) that needs to be notified of the results but need not necessarily to be consulted.

As it can be seen in the RASCI table, the Work Package Leaders are the main responsible for the identification of new risks, as well as its analysis and classification, Work Package Leaders will have the support of task leaders and partners from the same WP on these tasks.

Once the risks are identified and analysed, and a response plan for each is designed, they will be informed to the Project Coordinator who is the main responsible for the management of all risks identified in the course of the project.

4.1.1.3 Definitions of probability and impact

In order to proceed to the proper analysis of each identified risk, both probability and impact should be defined in the scope of the project.

Probability

The following scale will be used for the project in order to rate a risk probability properly:

Scale for Probability										
Rating	1	2	3	4	5	6	7	8	9	10
Interpretation	Low		Medium		Medium-High		High		Fact	

Table 18: Scale of Probability

As it can be seen on the table above, there are two numbers for each interpretation, meaning that inside each interpretation you have also degrees. For example, a risk with Low probability can be classified as "very low" (rating 1), or "low" (rating 2), and so on.

Impact

The table below show the types of impacts and its correspondent classification for the SMESEC project.

Impact on the schedule:

Impact	Classification
Delay of 3 or more months on DoA deadlines (tasks start/end time, deliverables and milestones deadlines) – i.e. Task 1.2 delay will have an impact on Task 3.4 start time by 3 months.	9-10
Delay of 2 months on DoA deadlines (tasks start/end time, deliverables and milestones deadlines)	7-8
Delay of 1 month on DoA deadlines (tasks start/end time, deliverables and milestones deadlines)	5-6
Delays on internal deliverables by 1 – 3 months	3-4
Delays on any task or deliverable that does not have impact on other tasks	1-2

Table 19: Impact on Schedule

Impact on the achievements of results:

Impact	Classification
One main objective of SMESEC not achieved, i.e. major impact on DoA, which could lead to an amendment request on the Grant Agreement	9-10
WP objective not fully achieved	7-8
Objectives of more than one Tasks are not achieved	5-6
Task objective not achieved	3-4
Task objective not fully achieved	1-2

Table 20: Impact on results

4.1.1.4 Risk Register

The Risk Register is the main result of the Risk Management Process, as it aims to reflect the output of many processes such as Identify Risks and Risk Analysis among others.

This document will be filled through various iterations, having as the main responsible for its management the Project Coordinator.

A separated spreadsheet will be provided for the consortium to this end. The Risk Register has the following fields:

Item	Description
Risk ID	The identification for each risk. i.e. R01, R02
Risk	The risk stated in a complete sentence which states the cause of the risk, the risk, and the effect that the risk causes to the project.
Risk Category	Categorization of risks by area of project affected, source of risk or other useful category.

Item	Description
WP related	WP number from which the risk belongs
Probability	The likelihood that a risk or opportunity will occur (check section 4.1.1.3 for more info on the values accepted).
Impact	The impact of the risk on the project if the risk occurs (check section 4.1.1.3 for more info on the values accepted).
Risk Score	Determined by multiplying probability and impact (scale from 0 to 100).
Risk Ranking	A priority list which is determined by the relative ranking of the risks (by their scores), within the project with the number one being the highest risk score.
Risk Response	The action which is to be taken if this risk occurs.
Trigger	Description of an event (or events) that will cause the risk to materialize. Risk Owners should be aware of this information in order they known when to take action.
Risk Owner	The person who the project manager assigns to watch for triggers, and manage the risk response if the risk occurs.
Risk Materialized (Y/N)	Information if the risk has already happened. (YES or NO)
Status after Response	After the risk response took place, the status should be described.
Overall Status (Open/Closed)	All risks after inserted in the risk register will have the Overall status "open". In case a risk no longer can occur (no longer exists) it should have the status "closed".

Table 21: SMESEC Risk Register Fields

As an example we provide below, in Table 22 (bear in mind this will be compiled in an excel file), a risk of the project (not real) to be used for helping in understanding what information must be provided for a risk:

Risk Identification				Qualitative Rating				Risk Response			Control		
Risk ID	Risk	Risk Category	WP Related	Probability	Impact	Risk Score	Risk Ranking	Risk Response (Avoid/Mitigation)	Trigger	Risk Owner	Risk Materialized Y/N	Status after Response	Overall Status (Open/Closed)
R01	Problem for satisfying a GDPR-related risk. One partner provided as mandatory for them as risk related to the GDPR which we cannot fulfil in the project. We could have listed a requirement that could not be fulfilled endangering the evaluation of the project.	Scope	WP2	2	7	14	1	Avoid: check the reports of requirements of the use case weekly/monthly meetings and inform use case partners about the boundaries of the solutions to be developed in the project.	Deliverable 2.1 describes the requirements of a use case partner related to the GDPR. This will happen by M6.	ATOS	N		

Table 22: SMESEC Risk Register File

4.2 Identify Risks

The main output of this process is the list of risks identified by the consortium. Work Package Leaders should provide the project coordinator the following information for this process:

- Risk ID
- Risk
- Risk Category
- WP related

The Project Coordinator will be in charge of coordinating this process, ensuring that the required level of detail of the risks identified is present.

The project should use as starting point the risks that are already present in the DoA.

As all processes inside the Risk Management Process, this is an iterative process that will take place through the project lifetime. All WP leaders are responsible for a regular overview on new risks that could take place and were not foresaw during the start of the project. These new risks should be informed to the Project Coordinator as soon as they appear.

The Project Coordinator also will ensure that a regular communication channel will be open for this end through teleconferences and e-mails (or other communication tools provided).

The Project Coordinator will also regularly inform the consortium of the status of the Risk Register, informing of any new risks found its impact and the responses agreed.

4.3 Risk Analysis

Before the project can plan any response for the identified risks, it is needed a previous classification of each risk. This classification will be done through an analysis made by WP Leaders, where each risk will be given an impact and probability. Please check sub-section 4.1.1.3 for further details on how to classify each risk.

The following columns will be filled in this process:

- Probability
- Impact
- Risk Score (computed by multiplying impact and probability)
- Risk Ranking (highest equals major risk)

4.4 Plan Risk responses

After the risk analysis takes place, the consortium has the sufficient information to provide responses for each risk identified.

For all identified risks, these are the responses that should be given:

- Responses to eliminate the threats before they happen (Avoiding actions)

- Responses to decrease the probability and/or impact of threats (Mitigation actions)

These are the columns to be filled in this process:

- Risk Response (Avoid / Mitigation)
    - Avoid: in case an identified risk could be eliminated, the consortium should then inform on this column of the measures to be taken for it (i.e. a risk of not reaching a specific deadline could be terminated if this deadline is changed).
    - Mitigation: in case a risk cannot be eliminated by the moment of its identification and analysis, a contingency plan should be provided along with measures to minimize the probability/impact
- Trigger: an event expected to cause the risk to occur. The risk owner should be aware of this information.
- Risk Owner: Person who will be responsible for the implementation and closure of the mitigating actions assigned to the risk.

It is very important to notice that when planning a response for a risk, the response could also generate a new risk. If this happens, this new risk (called Secondary Risk) should also be noted in the risk register.

4.5 Control Risks

The Project Coordinator will start this process after the project produced a full risk register, with all risks identified, their impact and probability assigned and also all planned responses described.

Control Risks process main goal is to ensure that all risks identified are properly handled by the consortium, as well as to ensure that any new identified risks are updated in the risk register.

The Project Coordinator, Work Package Leaders and risk owners should monitor the risk triggers and the status of all risks. Any new identified risks should be analysed and follow the same process as described in this plan (e.g. identification, analysis, plan risks responses, etc.).

Work Arounds

This process also could include the sporadically need of workarounds. Whether a risk that was not previously identified by the consortium materializes, the project should come up with a workaround for this risk and it should also be added to the risk register.

Closing Risks

The Project Coordinator is also responsible for closing risks that are no longer applicable. Any risk that is closed should remain in the risk register.

Main output

The main output of this process will be the data provided in the following columns in the risk register (although others columns could be updated if needed):

- Risk Materialized (Y/N): Information if the risk has already happened.

- Status after Response: In case the response took place, the status of the risk should be stated
- Overall Status (Open/Closed): All risks after inserted in the risk register will have the Overall status "open". In case a risk no longer can occur, it should have the status "closed".

When it happens

Finally, this is an iterative process that should be present on the day-to-day life of the project.

In all PMB project meetings (physical or remote) there will be a specific slot for the status of the risks as presented here.

If any new risk or update of an existing risk is identified, the Work Package leader should be notified immediately and start the process for compiling the information of the risk as described in section 4.

Following, the Work Package Leader will notify the PC and provide the information of the risk for updating the Risk Register.

4.6 Common Risk Management Errors

The following is a list of common risk management errors that all partners should be aware when managing risks:

- Risk identification is finished without a fully technical knowledge of the technical project goal.
- Identification done in a very short period of time, resulting in a very short list of identified risks or not enough information for them.
- The risks identified are general, instead of SMESEC project specific risks.
- Risk management process is not given enough time or resources.
- Risk management process is not proper explained to the whole consortium.

5 Conclusions

The document aims at being a project execution handbook and a reference for all project consortium members for the entire project duration.

This document compiles definitions of the project government bodies, summarizes all the procedures to ensure a successful collaborative work within the project, describes the involved roles and tasks, and the tools and instruments available in the project in order to conduct the work towards meeting the project objectives with the highest possible quality level.

References

[1] SMESEC Consortium Agreement; https://repository.atosresearch.eu/owncloud/index.php/apps/files/ajax/download.php?dir=%2FSMESEC%2FWP7%2FContract&files=SMESEC_CA_v1.1_signed.pdf

[2] SMESEC DoA. Grant Agreement Annex I.

[3] SMESEC Grant Agreement; https://repository.atosresearch.eu/owncloud/index.php/apps/files/ajax/download.php?dir=%2FSMESEC%2FWP7%2FContract&files=Grant%20Agreement-740787-SMESEC%20(1).pdf

[4] RASCI Model; Link: http://www.rascimethode.nl/en/about-us/rasci, retrieved 2017/11/27.

[5] Project Management Institution (2004), *Project Management Body of Knowledge - PMBOK Guide*, Newton Square – PA Ingram International 2013.

[6] Gitlab.Link: https://about.gitlab.com/., retrieved 2017/11/27.

Annex I

			Design									Implementation & Integration									Adaptacion & Optimization						Validation								Assessment			
WP	Start	End	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30	M31	M32	M33	M34	M35	M36
WP1	1	36																																				
T1.1	1	36	D1.1					D1.2 D1.3																														
WP2	1	6						M1																														
T2.1	1	6						D2.1																														
T2.2	1	6						D2.2																														
T2.3	1	6						D2.3																														
T2.4	1	6																																				
WP3	1	36									M2									M3 M4						M5												M6 M7
T3.1	1	24									D3.1									D3.2						D3.3												
T3.2	7	18																		D3.3																		
T3.3	7	36																		D3.4																		D3.6
T3.4	22	36																																				D3.7
WP4	10	24																		M8						M9												
T4.1	10	24																		D4.1						D4.2												
T4.2	10	24																		D4.3						D4.4												
T4.3	10	24																		D4.5						D4.6												
T4.4	10	24																		D4.7						D4.8												
T4.5	19	24																								D4.9												
WP5	19	36																								M10			M11					M12				M13
T5.1	19	24																								D5.1												
T5.2	21	27																											D5.2										
T5.3	25	32																																D5.3				
T5.4	22	36																																				D5.4
T5.5	20	36																																				D5.5
WP6	1	36						M14																												M15		M16
T6.1	6	36						D6.1																												D6.5		
T6.2	1	36											D6.2													D6.3												D6.4
T6.3	6	36																																				
WP7	1	36						M17																														M18
T7.1	6	36						D7.1						D7.2												D7.3												D7.4

Figure 7: SMESEC's Gantt Chart