COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

D6.3 Communication & Dissemination Plan (v2)

Work Package:	WP6		
Lead partner:	INOV INESC Inovação (INOV)		
Author(s):	Nelson Escravana, Vanessa Moreira (INOV), Danaja Fabcic Povse (KUL), Luigi Sgaglione (CINI), Alexander Krock (BIT), Cornelia Gerdenitsch (AIT), Barbara Pirillo (ENG), Ricardo Madeira Simões (CMA), Ion Larrañaga (S21SEC), Paco Abal (DSS), Almerindo Graziano (SIL), Pamela Lama (BOL), Sandro Mari (ISCOM), Giuliano Gugliara (CDA)		
Due date:	31st July 2018		
Version number:	1.0	**Status:**	Final

Grant Agreement N°:	740712
Project Acronym:	COMPACT
Project Title:	COmpetitive Methods to protect local Public Administration from Cyber security Threats
Call identifier:	H2020-DS-2016-2017
Instrument:	IA
Thematic Priority:	Secure societies – Protecting freedom and security of Europe and its citizens
Start date of the project:	May 1st, 2017
Duration:	30 months

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Horizon 2020
European Union Funding
for Research & Innovation

Project co-funded by the European Commission under the Horizon 2020 Programme.

Revision History

Revision	Date	Who	Description
0.1	20/04/2018	INOV	Table of Contents
0.2	02/07/2018	INOV	First version
0.3	03/07/2018	KUL	Additional contributions
0.4	06/07/2018	CINI	Additional contributions
0.5	09/07/2018	BIT, AIT	Additional contributions
0.6	10/07/2018	ENG	Additional contributions
0.7	12/07/2018	CMA	Additional contributions
0.8	17/07/2018	S21SEC	Additional contributions
0.9	19/07/2018	DSS, SIL	Additional contributions
0.10	19/07/2018	BOL, ISCOM	Additional contributions
0.11	20/07/2018	CDA	Additional contributions
0.12	20/07/2018	INOV	Pre-final version for internal review
0.13	28/07/2018	INOV	Consolidated version

Quality Control

Role	Date	Who	Approved/Comment
Internal Reviewer	23/07/2018	CINI	Approved with minor revisions
Internal Reviewer	28/07/2018	SIL	Approved

Disclaimer:

This document has been produced in the context of the COMPACT Project. The COMPACT project is part of the European Community's Horizon 2020 Program for research and development and is as such funded by the European Commission. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Table of Contents

List of Tables

Definitions and acronyms

CC	CyberConnector
CyberConnector	An internal knowledge collaboration site and social network that is used to share all the information among partners. Referred to also as CC.
DoA	Description of Action
MST	Management and Support Team
PC	Project Coordinator
SC	Scientific Coordinator

Executive Summary

This deliverable – D6.3 Communication & Dissemination Plan (v2) – sets the strategy to be developed in the next nine months [M16-M24] of the COMPACT project, following on the strategy defined previously in D6.2 Communication & Dissemination Plan (v1) [1] and the results reported in D6.4 – Communication and Dissemination Report (v1) [2]. As stated in the preceding plan, the communication and dissemination strategy of COMPACT is based on three strategic axis: Outreach/Awareness, Participation and Uptake/Advocacy, and this plan outlines the strategy for the second axes of Participation.

The document begins with an overview of strategic approach defined in the beginning of the project and the contribution of communication and dissemination to the overall project's objectives and KPIs. Still in the first section, we identify key audiences and messages to engage with COMPACT, based on the LPAs Community Model [3] [4].

Following upon this, the deliverable identifies the communication and dissemination opportunities and actions to be developed during the next stage of the project setting the foundations for the Uptake/Advocacy axes that should follow. COMPACT will continue to target strategic audiences through participation in scientific events and pursuing publishing opportunities, as well strengthen its participation in LPA and IT industry events as well as the organisation of targeted meetings to promote the project's results and engage audiences to participate in COMPACT through its Information Hub. It is also presented the main input of WP6 to the Information Hub through Task 6.3 –Best Practices and Guidelines for immediate adoption by LPAs and to be further developed in D6.5 and D6.8. Here we also present a list of related projects to potentially collaborate with within the scope of COMPACT.

The final sections of the document present the approach for monitoring and evaluating the strategy implementation and sets the rules for partners to follow in order to improve the communication among the consortium regarding the communication and dissemination activities developed.

1. Introduction

Deliverable 6.2. Communication & Dissemination Plan (v2) evolves the previous version that set out the overall strategic guidelines to be followed throughout the project development. Following within the scope of Work Package 6 – Task 6.1. Dissemination Planning and Implementation it is its main objective to ensure that COMPACT's developments and results are communicated to the relevant stakeholders. This version of the plan carries on the work developed so far in order to contribute for the following objectives:

- forge and maintain close contact with LPAs and other relevant stakeholders to inform them about the project;
- disseminate project results, publish results in peer-reviewed scientific journals and attend conferences and workshops;
- promote professional links between the consortium and external stakeholders to boost cooperation for the exploitation of the project results.

While the first version (D6.2) of the plan focused on defining general guidelines and actions to be implemented during the project's first year, this version outlines the actions for the next period (from M16 – August 2018 to M27 – July 2019) profiting from D6.4. – Communication and Dissemination Report and D2.4 and D2.11 – LPAs Community Model in order to fine-tune the Dissemination & Communication approach for the following stages of the project.

2. Strategic approach

As previously defined, based on COMPACT's high-level objectives the Communication and Dissemination Plan takes on a comprehensive approach involving target audience based on three strategic axes aligned: outreach/awareness, participation and uptake/advocacy.

Table 1 - Communication Strategic Axes

Outreach/Awareness			Objective #1 - Making the PA personnel aware of the basic cyber security threats they are exposed to.
	Participation		Objective #2 - Improving the skills – both technical and behavioural – of the PA personnel via innovative training techniques that are well received by the (non IT-expert) workforce.
			Objective #3 - Providing protection tools against basic cyber security threats, i.e. those with a higher impact on LPAs. These include: phishing, ransomware, Bring Your Own Device (BYOD), jailbreaking the cloud, cross-site scripting, code (particularly SQL) injection, and more.
		Uptake/Advocacy	Objective #4 - Creating a LPAs level information hub, for favouring reliable and timely exchange of information among LPAs on cyber security guidelines and best practices, as well as on Indicators of Compromise (IoC).
			Objective #5 - Creating a link between COMPACT LPAs level information hub and major EU level initiatives, for supporting LPAs to improve cyber-resilience in a complex European context.

2.1. From Outreach/Awareness to Participation and Uptake/Advocacy

During the first half of the project, the focus was on **Outreach/Awareness** to build project's outreach capacity and raise awareness for cybersecurity issues among strategic audiences and citizens. Although being considered for the whole duration of the project, this axis was particularly important during the first year as a way to pave the way to ensure a solid base for the second strategic axis that has started to have some expression from M13 – May 2018 with the beginning of targeted contacts with relevant audiences.

With the architecture definition and the beginning the development of the COMPACT Platform, we now fully enter the *Participation* axis of the project focusing on engaging LPAs/SMEs and IT services providers to cooperate with the project. **Participation**, along with **Uptake/Advocacy** towards the final months of the project, relies heavily on the development and animation of the Information Hub.

The Information Hub will be the centre for all audiences with an interest in COMPACT to share information and knowledge. Therefore, the communication strategy will focus on reaching a greater engagement level from specific audiences, with messages focusing on the benefits identified in WP2 – Scenarios, Human Factors, and Legal/Ethical Aspects, Task 2.4 – Modelling the Community of Local Public Administration.

The success of this stage will set the context for the final strategic axis of communication, **Uptake/Advocacy***,* to position COMPACT as a channel for IT suppliers to deploy new cybersecurity solutions and for LPAs to deal with complex cyber-threats. It will be paramount to engage the audiences as a foundation for the work to develop further in WP7 – Exploitation. and to ensure the platform's future and sustainability beyond the end of the project. Some of the work on this axis will start from M25 – May 2019 and will be the focus of D6.6 – Communication and Dissemination Plan (v3) to be submitted by M27 – July 2019.

2.2. Contribution to COMPACT's KPIs

As the project enters the Participation axis, it is important to analyse how the communication and dissemination plan contributes to the projects KPIs. As the table below shows, this axis is set based on the LPA community to be build much around the COMPACT Information Hub.

Table 2 - C&D contribution to project KPIs

Intention		Proportion	Deadline
Outreach / Awareness	Get peer-reviewed journal papers published	>=2	M30
	Get peer-reviewed conference papers published	>=4	M30
	Get general articles published	>=3	M30
	Get general press/magazines articles published	>2	M30
	Get website visitors	>2000	M30
	Get unique visitors to the website/information hub	>150	M30
	Have downloads of multimedia material on the website	>30	M30
	Have engagement in COMPACT's social media accounts	>=150 (followers/likes)	M30
	Get newsletter subscribers	>150	M30
	Get references of COMPACT in other websites	>40	M30
Participation	Have LPAs joining COMPACT information hub	>=10	M30
	Have country-level security stakeholders joining COMPACT information hub	>=3	M30
	Have EoI signed by external organisations for accessing COMPACT repository	>=10	M30
	Have EoI signed by external organisations for contributing to COMPACT repository	>=5	M30

Uptake / Advocacy	Have EU-level cybersecurity stakeholders actively involved in COMPACT information hub	>=5	M30
	Have best practices defined for immediate adoption by LPAs	>=20	M20-M30
	Have guidelines defined for immediate adoption by LPAs	>=20	M20-M30

Therefore, the plan presented in the following sections builds on some of the work developed so far in contacting targeted audiences to present COMPACT and its solutions. What is intended in the following months, and especially with the deployment of the COMPACT Information Hub, is to engage those audiences to become part of the COMPACT community.

2.3. The COMPACT audiences

Earlier in D6.2, key audiences and messages have been identified as follows:

Table 3 - COMPACT audiences

Audience	Messages focused on:
LPAs / SMEs	• Cybersecurity issues affecting organisations • Human error • Crime ware - Ransomware • Web Defacement • Social Engineering • Learning through gamification • Knowledge sharing – information hub • COMPACT's usability and automation
IT security / solutions providers	• "Cloud-enabled" and "Cloud-ready" solution • COMPACT's usability and automation • Technology Readiness Level
Research community	• Technology Readiness Level • Learning through gamification
Local national communities	• Cybersecurity risks in everyday behaviour

These have been the broader issues communicated about COMPACT and its environment, serving the strategic axis of **Outreach/Awareness**. Now that the project enters a stage of greater specification and definition it is important to adjust the strategy to in a more direct way engage the strategic audiences. For this, the plan will fall back on the work developed for the COMPACT community modelling according to which there have been identified specific groups of stakeholders [3] [4]:

Table 4 - COMPACT community stakeholders

Stakeholder	Description
Local Public Administration	EU local public authorities willing to tackle Cyber threats.
Central Public Administration & National Bodies	Central Public Administration willing to tackle cyber threats and relevant ministries dealing with cybersecurity. This group of stakeholders includes also law enforcement agencies, governmental institutions that enforce laws related to cyber offences or those perpetrated through cyber space.
EU Bodies	European bodies involved in, or closely related to, the definition of regulations affecting the cybersecurity field.
Legal Experts	Experts in the field of EU and national law supporting the community in order to guarantee that the COMPACT solutions comply with the EU and national legislations.
Solution Providers	Entities aiming to transfer solutions to production by creating and maintaining applications and services. It can be divided in two subgroups: • Cybersecurity Providers providing security-related services, products, and software focused on security for public authorities, and • System Integrators focusing on integrating security technologies in networks, systems, and applications.
Research	This group encompasses entities interested in finding new solutions, opposed to the Solution Providers. Therefore, it includes Universities, Research Institutes, EU initiatives, and EU Research Projects, among other possible temporary grouping of organisations.

2.3.1. Messages per audience

According to the key groups identified in the community model and the benefits identified by the all the partners, the communication messages will target the specific audiences. The main tools and services of COMPACT will be highlighted – Risk Assessment, Education, Monitoring, Knowledge Sharing – in a way to emphasise their specific benefits according to the groups/profile of stakeholders. This strategy will have a two-fold approach, having a first stage of providing motivations to join the COMPACT community, followed by the second stage of presentation of the benefits each group will add to the community. This two-fold strategy allows us to implement a holistic approach to the community giving answer to not only the question "how can you benefit from COMPACT community?", but also to how different stakeholders will contribute to build an active community, with shared interests in improving cybersecurity in Local Public Administration across Europe.

In this section, we build on the work developed in D2.11 LPAs Community Model (v2) with the identification of the benefits of becoming a member of the community and evolve them to specific messages to target each one of the identifies community audiences.

The following table sets the key messages to attract the identified groups of stakeholders by giving answer to the question “What can the COMPACT community give me?”

Table 5 - Key messages for potential members of the COMPACT community (I)

Stakeholder	**COMPACT Tool/Service**			
	Risk Assessment	Education	Monitoring	Knowledge Sharing
Local Public Administration	Information on the most recent cyber threats identified **increasing your knowledge and decision-making capabilities**. Access to the most recent technical information on identified cyber threats **increasing your awareness and preparedness to potential cyber-attacks**.	Training to increase **your awareness to cybersecurity issues and your day-to-day decision-making capabilities**. Information about COMPACT educational offers, suggestions and guidelines on how to plan cybersecurity trainings **improving your results from training initiatives**. Training on specific cybersecurity solutions **improving your technical skills**.	**Information about COMPACT's monitoring offer**. IoC and technical information about cyber threats, and **support to the adoption and usage of COMPACT's monitoring solution**.	Alerts on the latest cyber threats **increasing your preparedness and ability to avoid attacks in day-to-day activities**. Information on the latest regulations and policies on cyber and data protection **increasing your knowledge and decision-making capabilities**. Information about cybersecurity solutions beyond COMPACT **increasing your knowledge on the most recent solutions in the field**.

Central Public Administration & National Bodies		Information, by sector or by region, on LPA exposure to cyber threats **increasing your knowledge and decision-making capabilities**.	IoC and related information on cyber incidents at the local level for your further analysis **improving your preparedness and response capabilities**. Information, by sector or by region, about ongoing LPA training processes **increasing your knowledge on specific skills being developed in the field of cybersecurity.**	Access to a wide audience of LPA to inform on the most recent cyber alerts and news **improving the reach of your communications to the local level.** Feedback from LPA, legal experts, and EU bodies on current or upcoming regulations on cyber and data protection **increasing your knowledge and decision-making capabilities.**
EU Bodies		Information, by sector or by country, on LPA exposure to cyber threats **increasing your knowledge about LPA vulnerabilities, contributing to policy making.**		
Legal experts	Information on gaps in legal knowledge in the field of data protection, privacy and security **increasing your abilities to contribute to the development of the field.**	Possibility to explore innovative ways of resolving the privacy vs. security conflict and **adapt them to the real needs and requirements of LPAs**.		Access to a wide audience on the legal challenges of cyber security implementation **improving the effectiveness of your awareness campaigns for data protection, privacy and security issues.**

Solution Providers	Insight into the risks LPA faces in order to **design and offer solutions that are cost effective and improve the security posture of the LPAs**.	Feedback on training material being able to **improve it according to LPAS needs.** You will **extend your client user-base to LPAs.**	IoC and related information for further analysis and **improvement of your solutions/products**. Monitoring information about threats in other environments **increasing your possibilities to detect and protect against ongoing attacks in other clients.**	Promotion of your solutions/products in the LPA community possibly **extending your client-base.** Interact with other solution providers to integrate tools and services **increasing the impact of your own solutions/products.**
Research	Information, by sector or by region, on LPAs' exposure to cyber threat getting **valuable data for your own research**.	Promotion of high education training on cyber threats **supporting LPAs cyber-resilience improvement**.	IoC and related information for further analysis contributing for overall **improvement of the LPA community's preparedness and response capabilities.**	Access to a wide community of LPAs to inform about the latest research results **increasing the reach of your dissemination campaigns**. Suggestions about new topics from the community members **contributing to the development of your own research**.

Because the intention of COMPACT is to create a dynamic community based on shared interests, which ideally will continue to exist beyond the end of the project it is important that all audiences are also aware of how they can add value to the community. The following table describes de messages to attract members by answering the question "What can I bring to the community?"

Table 6 - Key messages for potential members of the COMPACT community (II)

Stakeholders	**COMPACT Tool/Service**			
	Risk Assessment	Education	Monitoring	Knowledge Sharing
Local Public Administration	Feedback on the risk assessment process. Consultancy on how to address cyber threats.	Feedback on attended training programmes. Feedback on COMPACT educational offer.	Feedback on COMPACT monitoring offer. IoC and technical information about threats.	
Central Public Administration & National Bodies	Consultancy on how to address cyber threats.		IoC and related information.	Alerts and news on the latest cyber threats at national and global levels. Information to the community about regulations at national level.
EU Bodies				Information about regulations and policies on cyber topics at EU level.
Legal experts	Consultancy on compliance with the GDPR and other regulations.	Training material on cyber security, privacy, and data protection legislation.		Promotion of compliance with legal regulations through conferences, workshops and consultancy.
Solution Providers	Support in the assessment of information and cybersecurity risks. Support in acquisition, deployment and integration of security solutions.	Training material on specific cybersecurity solutions.	IoC and related information for analysis. Managed security services including monitoring and reporting.	Information to LPAs about new solutions/products. Information on current threats. Best Practices. Threat intelligence and security feeds.

Research	Consultancy on how to address cyber threats.	Training material on cyber threats.	Ioc and related information for analysis.	Information on the latest research results. Suggestions about new lines of research.

3. Communication and Dissemination actions

Communication and dissemination actions are identified throughout the project all partners involved in COMPACT. There is a document available in CyberConnector for partners to update with potential opportunities and report on the activities developed.

3.1. Scientific Publications and Conference Presentations

COMPACT partners will continue to push for publication of scientific articles both in journals and in conferences. As the projects develops, more results will be available for dissemination, so it is expected that this activity will continue to grow following upon the already good results from the first year with three accepted conference papers (cf. D6.4 [1]).
Moreover, KUL has submitted a paper on GDPR relevance in cyber fields and AIT is preparing a paper on cyber secure behaviour in the workplace to submit soon, based on the work developed within Work Package 2.
A list of relevant conferences has been identified where partners may present project results:

Table 7 - List of potential events to present COMPACT results

Event	Type of event	Audience	Date	Location
14th Symposium on Usable Privacy and Security	Symposium	Academia and industry	Aug 12-14 (2018)	Baltimore, MD (USA)
27th USENIX Security Symposium	Symposium	Researchers, practitioners, system administrators and programmers	Aug 15-17 (2018)	Baltimore, MD (USA)
EGOV-CeDEM-ePart 2018 Conference	Conference	Individuals from academic and applied backgrounds as well as from business, public authorities, NGOs, NPOs and education institutions	Sep 3-5 (2018)	Krems (Austria)
EGOVIS 2018	Conference	Academia, public administrations, and industry	Sep 3-6 (2018)	Regensburg (Germany)

23rd European Symposium on Research in Computer Security (ESORICS)	Symposium	Researchers	Sep 3-7 (2018)	Barcelona (Spain)
21st International Conference on Networked-Based Information Systems (NBiS-2018)	Conference	Researchers	Sep 5-7 (2018)	Bratislava (Slovakia)
21st International Symposium on Research in Attacks, Intrusions and Defenses	Symposium	Academia, government, and industry	Sep 10-12 (2018)	Crete (Greece)
4th Annual European Public Sector Transformation Conference	Conference	Public Administration	Sep 18 (2018)	Brussels (Belgium)
Cyber Tech Italy	Conference	Industry	Sep 26-27 (2018)	Rome (Italy)
10th NordiCHI Conference	Conference	Researchers	Oct 1-3 (2018)	Oslo (Norway)
Cyber Security Europe	Conference	Industry	Oct 3-4 (2018)	London (UK)
6th Annual European Cybersecurity Conference	Conference	Policy makers	Nov 8 (2018)	Brussels (Belgium)
ITAPA International Congress	Congress	Public Administration	Nov 14-15 (2018)	Bratislava (Slovakia)
Central European Cyber Security Conference	Conference	Academia, public administrations, NGO's and industry	Nov 15-16 (2018)	Ljubljana (Slovenia)
Computers, Privacy and Data Protection conference[1]	Conference	Academia, public administrations, NGO's and industry	Jan 30 - Feb 1 (2019)	Brussels (Belgium)
IEEE International Conference on Computer Communications	Conference	Research Community	Apr 29 - May 2 (2019)	Paris (France)
International Conference on Human Factors in computing Systems (CHI)	Conference	Researchers and practitioners	May 4-9 (2019)	Glasgow (UK)
ACNS – Applied Cryptography & Network Security	Conference	Academia and industry	TBD	TBD

[1] COMPACT is preparing a panel on data protection and data security in public administration for the annual Computers, Privacy and Data Protection conference in Brussels, January 2019. The decision of the CPDP whether COMPACT's panel has been accepted will be communicated during summer of 2018.

3.2. Workshops

A second COMPACT Workshop will take place during the last year aiming for a broader audience than the one from the first workshop that focused on gathering requirements for the COMPACT solution and validating it.

The objective of the second workshop is to increase awareness and disseminate the project results to the wider LPA community. Therefore, COMPACT will identify conferences related to e-Government and cybersecurity happening during the last year of the project to host the COMPACT workshop.

Other workshops may be organised by partners at regional or national levels whenever considered relevant.

3.3. LPAs/SMEs events

COMPACT will target events related to Public Administration and e-Government in order to reach a larger number of organisations to present and promote the COMPACT results, especially during the demonstration phase of the project. Here we identify some Public Administration events where COMPACT may be presented.

Table 8 - List of potential LPA events to promote COMPACT

Event	Description	Partner
VIR Nordwest	Conference of IT officers from municipalities in North-Western Germany	BIT
Forum PA	Meeting on innovation and modernization of the Italian public administration, takes place in Rome, in the month of May.	CDA
SEMIC	The SEMIC conference is an annual international event bringing together policy makers, ICT solution developers, industry and researchers with a common interest in topics related to information exchange and management for public administration.	
Forum PA Emilia-Romagna	Forum designed to develop an ongoing confrontation among private stakeholders, LPAs and The Region Emilia-Romagna.	BOL
Events organised by the Eurocities' Knowledge Society Forum	The Eurocities' Knowledge Society Forum supports cities to ensure that all citizens can have access to ICTs and participate in the information and knowledge society and helps public administrations to make the most of the rapid development of new technologies.	BOL

3.4. IT industry events

Considering the potential of the COMPACT platform for integration of major COTS it is important to reach cybersecurity providers and system integrators in order to present the COMPACT solution. Here we identify some industry events where COMPACT may be presented.

Table 9 - List of potential IT industry events to promote COMPACT

Event	Description	Partner
Cyber Security Summit	One of the major cyber conferences in the UK bringing together industry's networking experts and penetration testers to share knowledge.	
InfoSecurity Europe	One of the biggest computer security conventions in Europe.	SIL
Cyber Security Europe	Cyber Security Europe offers invaluable security insight for both IT managers and security specialists. Experts share knowledge on how to build stronger defences against cyber-attacks and how to recover in case of breach.	
Regional Cybersecurity Summit	The Regional Cybersecurity Summit is an annual event organized by the ITU Arab Regional Cybersecurity (ARCC), which brings together decision makers from both the government and industrial sector. The event has a strong participation from all Arab countries, which are part of the ARCC and showcases security vendors from across a wide range of sectors and keynote talks from security experts	SIL

3.5. Targeted meetings

With the achievement of milestone 4 of the project – *First Integrated Platform and Trials Setup*, COMPACT will organise targeted meetings to be carried out during the demonstration phase. These targeted meetings will encompass encounters with **SMEs**, **medium to large corporate organisations**, and with representatives of **users at a local, regional and national level**.

The meetings are planned to contact directly potential organisations with interest in COMPACT and in becoming a member of the community.

3.6. Related R&I projects

COMPACT will continue to pursue collaboration, cooperation, and cross-fertilisation with other relevant EU-projects in order to promote its results and maximise its reach. A list of project is identified for partners to contact for potential collaboration opportunities.

Table 10 - Related R&I projects

Project	Description	Partner
CIPSEC Enhancing Critical Infrastructure Protection with innovative SECurity framework	The main aim of CIPSEC is to create a unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in IT (information technology) and OT (operational technology) departments of CIs. As part of this framework CIPSEC will offer a complete security ecosystem of additional services that can support the proposed technical solutions to work reliably and at professional quality. These services include vulnerability tests and recommendations, key personnel training courses, public-private partnerships (PPPs) forensics analysis, standardization and protection against cascading effects. All solutions and services will be validated in three pilots performed in three different CI environments (transportation, health, environment). CIPSEC will also develop a marketing strategy for optimal positioning of its solutions in the CI security market.	CINI
SISSDEN Secure Information Sharing Sensor Delivery event Network	SISSDEN is a project aimed at improving the cybersecurity posture of EU entities and end users through development of situational awareness and sharing of actionable information. It builds on the experience of Shadowserver, a non-profit organization well known in the security community for its efforts in mitigation of botnet and malware propagation, free of charge victim notification services, and close collaboration with Law Enforcement Agencies, national CERTs, and network providers.	
HERMENEUT Enterprises intangible Risks Management via Economic models based on simulatioN of modErn cyber-aTtacks	HERMENEUT assesses vulnerabilities of organisations and corresponding tangible and intangible assets at risk, taking into account the business plans of the attacker, the commoditisation level of the target organisations, the exposure of the target and including human factors as well as estimating the likelihood that a potential cyber-attack exploits identified vulnerabilities. HERMENEUT's cyber-security cost-benefit approach combines integrated assessment of vulnerabilities and their likelihoods with an innovative macro- and micro-economic model for intangible costs, delivering a quantitative estimation of the risks for an organisation or a business sector and investment guidelines for mitigation measures.	ENG
SAINT Systematic Analyzer in Network Threats	SAINT proposes to analyse and identify incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing. Analysis of the ecosystems of cybercriminal activity, associated markets and revenues will drive the development of a framework of business models appropriate for the fighting of cybercrime. The role of regulatory approaches as a cost benefit in cybercrime reduction will be explored within a concept of greater collaboration in order to gain optimal attrition of cybercriminal activities.	
NeCS European Network for Cyber-security	The European Network for Cyber Security (NECS) addresses the training and development of a European talent pool to help implement and support the European Cyber-security strategy2 as highlighted in the EC's Digital Agenda. Today there is a strongest need than ever to grow researchers that combine a strong academic foundation with practical experiences, technological expertise with awareness of the socio-economic and legal context and conviction to furthering research with an entrepreneurial spirit. The 4-year NECS project for a cyber-security research and training network makes a significant contribution towards meeting the increased demand of human expertise in this critical field.	

CANVAS Constructing an Alliance for Value-driven Cybersecurity	The growing complexity of the digital ecosystem in combination with increasing global risks entail the danger that enforcing cybersecurity may bypass other fundamental values like equality, fairness or privacy, whereas downplaying cybersecurity would undermine citizens' trust and confidence in the digital infrastructure. For tackling this challenge, the European Commission has chosen the CANVAS Consortium – Constructing an Alliance for Value-driven Cybersecurity – to unify technology developers with legal and ethical scholar and social scientists to approach the challenge how cybersecurity can be aligned with European values and fundamental rights. Within three years, CANVAS aims to bring together stakeholders from key areas of the European Digital Agenda – the health system, business/finance, and law enforcement/national security – for discussing challenges and solutions when aligning cybersecurity with ethics. A special focus of CANVAS is on raising awareness on the ethics of cybersecurity through teaching in academia and industry.	
DISIEM Diversity Enhancements for SIEMs	Security Information and Event Management (SIEM) systems are a fundamental component of the ubiquitous ICT infrastructures that form the backbone of our digital society. These systems are mostly used to monitor infrastructures using many types of sensors and tools and correlate the obtained events to discover possible threats (attacks, vulnerabilities, etc.) to the organization. The DiSIEM project aims to enhance existing SIEM systems with diversity-related technology. More specifically, the project wants to enhance the quality of events collected using a diverse set of sensors and novel anomaly detectors, to add support for collecting infrastructure-related information from open-source intelligence data available on diverse sources from the internet, to create new ways for visualising the information collected in the SIEM and provide high-level security metrics and models for improving security-related decision project, and allow the use of multiple storage clouds for secure long-term archival of the raw events feed to the SIEM. Given the high costs of deployment of SIEM infrastructures, all these enhancements will be developed in a SIEM-independent way, as extensions to currently available systems, and will be validated through the deployed in three large-scale production environments.	
KONFIDO Secure and Trusted Paradigm for Interoperable eHealth Services	KONFIDO is a H2020 project that aims to leverage proven tools and procedures, as well as novel approaches and innovative technology, in view of creating a scalable and holistic paradigm for secure inner- and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way both at national and European levels.	CINI
EU-SEC The European Security Certification Framework	The European Security Certification Framework (EU-SEC) strives to address the security, privacy and transparency challenges associated with the greater externalisation of IT to Cloud services. EU-SEC will create a certification framework under which existing certification and assurance schemes can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the Cloud. It will be tested and validated in pilots involving industrial partners.	

FORTIKA **Cyber Security Accelerator for trusted SMEs IT Ecosystems**	FORTIKA aims to minimise the exposure of small and medium sized businesses to cyber security risks and threats, and help them successfully respond to cyber security incidents, while relieving them from all unnecessary and costly efforts of identifying, acquiring and using the appropriate cyber security solutions. To fulfil its vision the project adopts a security by design hybrid approach that adequately integrates hardware and software with business needs and behavioural patterns at individual and organisational level.	
SMESEC **Protecting Small and Medium-sized Enterprises digital technology through an innovative cyber-SECurity framework**	SMESEC consortium is proposing to develop a cost-effective framework composed of specific cyber-security tool-kit 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; for this consortium, it is important that SMEs do not only look at cyber-security as an obstacle, but also they understand the business opportunity beyond it.	
CS-AWARE **A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis**	The project proposes a cybersecurity situational awareness solution for local public administrations, which, based on an analysis of the context, provides automatic incident detection and visualization, and enables information exchange with relevant national and EU level NIS authorities like CERTs. Advanced features like system self-healing based on the situational awareness technologies, and multi-lingual semantics support to account for language barriers in the EU context, are part of the solution.	
certMILS **Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats**	certMILS develops a security certification methodology for Cyber-physical systems (CPS). CPS are characterised by safety-critical nature, complexity, connectivity, and open technology. A common downside to CPS complexity and openness is a large attack surface and a high degree of dynamism that may lead to complex failures and irreparable physical damage. The legitimate fear of security or functional safety vulnerabilities in CPS results in arduous testing and certification processes. Once fielded, many CPS suffer from the motto: never change a running system. certMILS increases the economic efficiency and European competitiveness of CPS development, while demonstrating the effectiveness of safety & security certification of composable systems.	
FENTEC **Functional Encryption Technologies**	Functional encryption (FE), has been recently been introduced as a new paradigm of encryption systems to overcome all-or-nothing limitations of classical encryption. In an FE system, the decryptor deciphers a function over the message plaintext: such functional decryptability makes it feasible to process encrypted data (e.g. on the Internet) and obtain a partial view of the message plaintext. This extra flexibility over classical encryption is a powerful enabler for many emerging security technologies (i.e. controlled access, searching and computing on encrypted data, program obfuscation…).	

DOGANA **aDvanced sOcial enGineering And vulNerability Assessment**	The advent of Social Networks has made both companies and public bodies tremendously exposed to the so-called Social Engineering 2.0, and thus prone to targeted cyber-attacks. Unfortunately, there is currently no solution available on the market that allows neither the comprehensive assessment of Social Vulnerabilities nor the management and reduction of the associated risk. DOGANA aims to fill this gap by developing a framework that delivers "aDvanced sOcial enGineering And vulNerability Assessment". The underlying concept of DOGANA is that Social Driven Vulnerabilities Assessments (SDVAs), when regularly performed with the help of an efficient framework, help deploy effective mitigation strategies and lead to reducing the risk created by modern Social Engineering 2.0 attack techniques.	ENG
MISP **An Open Source Platform for Threat Intelligence**	MISP is A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Storing and especially using information about threats and malware should not be difficult. MISP is there to help you get the maximum out of your data without unmanageable complexity. The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators. The platform is funded under the Connecting Europe Facility.	SIL

3.7. Media Relations

Relations with the media will gain relevance in COMPACT as the project initiates *Validation and Demonstration in Operational Environment* (WP5). Partners will ensure that the online demonstrations of project outputs are prominently featured issuing press releases in local languages for their local press and their local MEP.
After the releases, partners will pursue publication of interviews and articles, as well as meeting with their local MEP to raise awareness for the impact of EU funds at local level.
Joint press releases are scheduled according to the projects milestones:

- PR4 – November 2018
- PR5 – May 2019
- PR6 – August 2019
- PR7 – November 2019 (project conclusion and evaluation)

3.8. Best Practices and Guidelines

Task 6.3 *Best Practices and Guidelines for immediate adoption by LPAs* focuses on the collection and refinement of input for the definition of Best Practices and Guidelines for LPAs. It includes collecting success stories and best practices from national and international experts and end-user groups. This task is closely linked to the COMPACT Information Hub.

3.8.1. The COMPACT Information Hub

The COMPACT Information Hub will accompany all phases of the development of the COMPACT solution.

Mainly, the Information Hub will enable the community to share updated information about the latest cyber threats and to share Indicators of Compromise (IoC) related to the new cyber threats. In addition, the COMPACT Information Hub will enable sharing, commenting and reviewing rules that each LPAs can adopt immediately. The Information Hub will serve the first objective of the community, that is to enhance the understanding of the system in which the COMPACT project operates.

Task 4.4 *Community Tool and User Profile* is the task dedicated to the actual development of the community tool. After the first release of the platform on M18, the Information Hub will follow a process of continuous validation and adaptation in order to guarantee full alignment with users' needs and feedback, gathered in the context of WP5 activities.

The Information Hub will also be an instrument of exploitation enabling direct communication with public administration sector and relevant parties.

In terms of planning, a number of best practices will be collected from the LPAs already involved in the project and then, once the Information Hub is released, best practices will be used and published by other LPAs and relevant stakeholders who join the Hub.

Particularly, in line with Objective #4 and with the KPIs expressed by the DoA, and reported in this document, a number of >=20 best practices for immediate adoption by LPAs will be defined and published by the end of the project (M30).

To ensure regular updates the project partners will be contacted bi-weekly by BIT as responsible partner for T6.3 *Best Practices and Guidelines for immediate adoption by LPAs* as a reminder to supply content for sharing on the Information Hub. This content will be the best practices from the LPAs but also warnings about new cybersecurity threats encountered by the LPAs to make it easier for other LPAs to identify those threats, e.g. new scam-mails.

It is essential that all partners contribute to the information hub, as BIT by itself can only report about best practices from Bremerhaven. This is content reported by the partners not created by BIT.

4. Promotional instruments

4.1. Newsletter

There was developed a newsletter to communicate with project stakeholders throughout the project. A new issue is released every six months to inform relevant audience on the project status and its news and developments. For the following period, there are planned 3 more issues:

- Newsletter no. 3 – May / October 2018
- Newsletter no. 4 – November 2018 / April 2019
- Newsletter no. 5 – May / October 2019

4.2. Blogs

COMPACT takes a proactive approach through the partners to take part in relevant blogs in order to promote the project's visibility and reach.

Table 11 - List of blogs to promote COMPACT

Blog	Partner
KU Leuven CiTiP	KUL
INSIDE inside.eng.it	ENG
S21SEC blog	S21SEC
Kaspersky blog	KSP

4.3. Multimedia

During the first half of the project, the consortium has produced two infographics to support communication actions focusing on general cybersecurity issues affecting LPAs. In order to support the two last strategic axes of the plan, more multimedia, such as leaflets and videos, are to be produced, based on the specific messages for the different stakeholder groups. These materials will be designed and adapted to the different channels of communication available to COMPACT like the project website or its social networks.

5. Contribution of partners to C&D

Partner	Contribution
ENG	ENG will leverage on its expertise and on its consolidated network — built during the participation to an array of European Research projects — to disseminate project results and main achievements. ENG will disseminate both internally (to its own work force) and externally. At the internal level, ENG is interested in developing in-house sessions in which it will exploit the gaming approach of COMPACT to improve the overall awareness and uptake of cyber-security “safe” strategies for its personnel. It will also channel this to contribute to the cyber-security course already taking place at its IT school. In order to reach out the audiences identified in this deliverable, ENG will make active use of institutional social media channel such as Twitter at EngineeringSpa that counts more than 4,136 followers and of the public website, as appropriate, increasing project visibility and raising interest from potential stakeholders. Publications of blog posts on the institutional channel INSIDE (https://inside.eng.it/) is also foreseen whenever there is the need to disseminate relevant projects results. ENG will also support • the animation of the COMPACT Twitter channel; • the organisation of events focused on stakeholders enlargement (potential users); • the engagement of selected stakeholders • the design and creation of dissemination material as appropriate.
CINI	CINI confirms the plans presented in the D6.2, that for convenience are reported below.

	CINI dissemination activities will cover academic as well as more general-purpose communication events (targeting the public at large). Internal knowledge dissemination: Throughout the project, internal partner workshops and annual symposia under participation of all project members (researchers, research advisors, mentors) will be held. These workshops will ensure the efficient distribution of knowledge among all partners, enable the definition of future research directions and be used to devise solutions to project challenges. CINI plans to disseminate COMPACT results internally through specialized training programs for PhD students enrolled in programs specifically related to cyber-security. External dissemination: Publication of research outcomes at scientific conferences and workshops and in renowned international journals at regular intervals. In particular, the publications shall focus on the applied scientific methods and the developed concepts that will solve the identified research challenges. At the conferences, a scientific validation of the conducted research will be obtained from discussions with the scientific audience and knowledge transfer is expected to emerge from the exposure of the works to leading international scientists.
INOV	INOV will continue to participate in local workshops and possibly organise one for national LPA in order to promote COMPACT's results and engage stakeholders facilitating fast adoption of the project results.
SIL	Silensec has a strong social media presence with nearly 100,000 followers on Facebook and nearly 5,000 on Linkedin. Silensec's contribution to the C&D will leverage the company's social media presence but also focus on the tradeshow events in Europe but also in the Middle East where the company operates
S21SEC	S21sec will disseminate the progress and results of the project using its existing marketing channels, such as social networks, press releases and both the corporate web page and blog.
ISCOM	ISCOM will disseminate the project's activities and results through the institutional website. ISCOM will organize a workshop in which the project activities will be presented together with the other research cyber security activities ISCOM is conducting.
AIT	Publishing at scientific conferences and in scientific journals. Press release in Q3 for the projects *Compact*, *Dogana* and *SecLearn*
KUL	Publishing in scientific journals. Participation in conferences and workshops. Promotion of COMPACT through CITIP blog and social media channels.
KSP	KSP confirms the plans presented in the D6.2 that for convenience are reported here. KSP will disseminate internally to its employees (around 3500 worldwide) through an internal newsletter that will include a description of COMPACT and KSP efforts in terms of security intelligence services (data feeds) and gamification approach to security awareness trainings. Moreover, KSP will publish press releases in order to disseminate COMPACT externally.
CMA	Promotion of COMPACT in CMA's social networks, website and intranet. Dissemination of cybersecurity awareness material among workers.

	Internal training sessions.
CDA	CDA will disseminate the evolution of the COMPACT project using videos, website and intranet. CDA will improve staff awareness of cyber-security by videos tutorial.
BOL	The Municipality of Bologna carries out dissemination and communication actions by promoting COMPACT in specific events related to LPA's as well as by presenting COMPACT throughout social media (e.g. Iperbole civic network and its social media channels such as FB and Twitter). In particular, updates on the project will be provided at the Iperbole section specifically dedicated to EU funded projects and through the international projects page on FB. At regional level COBO will share the project's outcomes within the Emilia-Romagna Community Network (CN-ER) that is the most important platform where Emilia Romagna's LPAs implement tools aimed at improving the field of digital administration. Internally, specific training sessions and dissemination of cybersecurity awareness material among workers will occur and updates on the projects will be given through the municipal Intranet
DSS	DSS is in touch with EUDEL (Association of Basque Country LPA's) to keep them informed with the progress of COMPACT. DSS has also sent mails to other important Spanish LPA's to introduce them COMPACT. San Sebastian local newspapers have also referred COMPACT in the previous months.
BIT	Article on city portal (Bremerhaven.de), posts on Facebook page of Bremerhaven and on the BIT company Facebook page, access to the newsletter of the Major Cities IT Users group (about 1600 recipients).

6. Monitoring and Evaluation

The work developed by the consortium within WP6 will continue to be monitored using the *3 O's Metrics* approach for measurement of results:

- Outputs – communication and dissemination efforts
- Outtakes – direct results of the efforts
- Outcomes – awareness/attitude/behaviour expressions of change towards the subject

Output	Outtake	Outcome
Peer-reviewed journal papers submitted	Peer-reviewed journal papers published/presented >=2	• Number of readers/attendees
Peer-reviewed conference papers submitted	Peer-reviewed conference papers presented/published >=4	• Number of readers/attendees
Participation in research events	Number of attendees	• Information queries • Media coverage – COMPACT mentions
Presentations at industry events	Number of attendees	• Information queries • Media coverage – COMPACT mentions

Presentation of results at LPAs / PAs events >=5	Number of organisations / attendees	• Number of information queries • Media coverage – COMPACT mentions
Organisation of events (workshops / seminars / conferences / …)	Number of organisations / attendees	• Information queries • Media coverage - publications and tone • Social media engagement - reactions, follows, comments, shares
Website development and update Website languages >1	Website visitors >2000	• Information queries • Shares • Downloads of multimedia material on the website >30
	Unique visitors to the website/information hub >150	
Press releases >=10	Publications in the media	• Contacts for articles/interviews
	Open PRs on the website	
Press releases delivered to traditional media >2	General press/magazines articles published >2	• Contacts for articles/interviews
Newsletters >=5 (every 6 months)	Organisations receiving e-newsletter >=120	• Publications • Information queries • New subscribers
	Open NLs on the website	
	Open/read NLs (e-mail)	
Public demos >=10	Attendees at public demos >=100	• Information queries • Media coverage – publications and tone • Social media engagement - reactions, follows, comments, shares
Contacts with selected audiences (e.g. LPAs managers)	Presentations to selected audiences >=20	• Information queries
Contacts with EU-level cybersecurity entities	EU-level cybersecurity hub presentations >=15	• Information queries from EU-level cybersecurity stakeholders
Contacts with SMEs	Meetings with SMEs >5	• Information queries from SMEs
Contacts with medium to large corporate organisations	Meetings with medium to large corporate organisations >5	• Information queries from medium to large corporate organisations

Contacts with representatives of users at a local, regional, and national level	Meetings with representatives of users at a local, regional, and national level >5	• Information queries from representatives

To monitor communication and dissemination actions of COMPACT:

- Definition of Google alerts with related search keywords;
- Website statistics – further developed in D6.1. – Website and Logo (report);
- Proactively monitoring presence on social media (Social Analytics);
- Partners' feedback on contacts after activities (workshops, conferences, meetings, etc.);
- Newsletter analytics.

7. Rules for C&D

In order to improve communication between the partners in the consortium concerning Communication & Dissemination, a WP6 dedicated team is created to streamline the process of reporting. As such, each partner defines a privileged point of contact to communicate with the WP6 leader. This contact receives requests from the WP leader and directs them internally, according to the topic at hand, and will be responsible for gathering information on the activities developed and report it on a monthly basis, as well as a plan of activities for the following month. The point of contact is also responsible for communicating any deviations from the plan as soon as possible.

Partner	Point of Contact
ENG	Barbara Pirillo
CINI	Luigi Romano
INOV	Vanessa Moreira
SIL	Almerindo Graziano
S21SEC	Ion Larrañaga
ISCOM	Sandro Mari
AIT	Cornelia Gerdenitsch
KUL	Danaja Fabcic Povse
KSP	Nadezhda Ilina
CMA	Ricardo Madeira Simões
CDA	Vincenzo Alaia
BOL	Rosanna Vallarelli
DSS	Paco Abal
BIT	Alexander Krock

The Input and Monitoring document is permanently available in CC for all partners to share opportunities for promoting COMPACT and to follow the activities developed by all the partners.

8. Conclusions

Considering the COMPACT's overarching objective of enabling LPAs to become the main actors of their own cyber-resilience improving process the communication and dissemination strategy aims to reach and engage as many European LPAs as possible so that their participation can contribute to a better COMPACT solution to be exploited beyond the conclusion of the project.

COMPACT has focused on the first strategic axes of Outreach/Awareness during the first year of the project and will now execute the Participation axes engaging LPAs and other project's stakeholders across Europe to take part in COMPACT, especially through its Information Hub. Through collaboration among the consortium, as well as through individual initiatives, the defined strategy now defined aims to target specific audiences focusing on the benefits of the COMPACT solution of effective tools and services for removing security bottlenecks.

This version of the deliverable focuses mainly on the second axis of the strategy – Participation. There is one more version of the Communication and Dissemination Plan that will build on this one as the projects develops and enters a stage of Uptake/Advocacy where the project's participants become ambassadors for COMPACT.

9. References

[1] D6.2 Communication & Dissemination Plan (v1)

[2] D6.3 Communication & Dissemination Report (v1)

[3] D2.4 LPAs community model (v1)

[4] D2.11 LPAs community model (v2)