COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

D6.2 Communication & Dissemination Plan (v1)

Work Package:	WP6		
Lead partner:	INOV INESC Inovação		
Author(s):	Nelson Escravana (INOV), Vanessa Moreira (INOV), Alexander Krock (BIT), Daniela Messina (CINI), Luigi Romano (CINI), Salvatore D'Antonio (CINI), Veronique Pevtschin (ENG), Danaja Fabcic Povse (KUL), Sandro Mari (ISCOM)		
Due date:	October 2017		
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	30/09/2017	INOV	Initial draft
0.2	11/10/2017	BIT, ENG, CINI, ISCOM	Additional contributions
0.3	13/10/2017	KUL	Additional contributions
0.4	18/10/2017	INOV	Integration of contributions and submission for internal quality check

Quality Control

Role	Date	Who	Approved/Comment
Internal Reviewer	24/10/2017	CINI	Approved with comments
Internal Reviewer	26/10/2017	SIL	Approved with comments

Disclaimer:

Table of Contents

List of figures

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
LPA	Local Public Administration
IoC	Indicators of Compromise
PA	Public Administration
SQL	Structured Query Language
BYOD	Bring Your Own Device
EoI	Expression of Interest

1. Introduction

As described in COMPACT's DoA [1], deliverable 6.2. registers the communication and dissemination strategies to follow and actions to take throughout the project. This deliverable falls within the scope of *Work Package 6 – Task 6.1 Dissemination Planning and Implementation* set out to ensure that COMPACT's results are disseminated and communicated to the appropriate target communities, at appropriate times, and through appropriate methods.
The objective of this task is to develop and promote means to raise awareness among interested parties and communities potentially impacted by COMPACT's outcomes. Therefore, these activities will focus on defining techniques and media for fostering project results, targeting specific audiences that can benefit from COMPACT's results, informing relevant stakeholders on the project's results, and participating in relevant initiatives in order to guarantee a wide visibility of the project's objectives and outcomes.

COMPACT's communication and dissemination objectives are:

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

This first version – Deliverable 6.2 (v1) – sets out the overall strategy for Communication and Dissemination throughout the project. The focus at this point is to define the strategic guidelines for the entire project and to outline actions to be developed in the first half of the project (until M15 – July 2018).

2. Strategic Approach

The goal of Work Package 6 is to support COMPACT's development by designing, implementing, monitoring, and evaluating a plan where communication plays a strategic role in the overall project success.
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: outreach/awareness, participation and uptake/advocacy.
These strategic axes are intended to guide the development and implementation of communication and dissemination actions throughout the project accordingly to the different evolution stages and are aligned with COMPACT's high-level objectives.

Table 1 – Communication Strategic Axes

<table>
<tr><td rowspan="5">Outreach/Awareness</td><td rowspan="1"></td><td rowspan="3"></td><td>Objective #1 - Making the PA personnel aware of the basic cyber security threats they are exposed to.</td></tr>
<tr><td rowspan="4">Participation</td><td>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.</td></tr>
<tr><td>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.</td></tr>
<tr><td rowspan="2">Uptake/Advocacy</td><td>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).</td></tr>
<tr><td>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.</td></tr>
</table>

- COMPACT Outreach/Awareness - **Build project's outreach capacity and raise awareness for cybersecurity issues**

The first strategic axis aims to build outreach capacity and raise awareness for cybersecurity issues and COMPACT's solutions among strategic audience and citizens. Communication and dissemination efforts will focus on information of benefits and expected/actual results presented through scientific publications and presentations at specialised conferences and PAs events, as well as activities of agenda setting. This axis is most relevant in the first year of the project as the focus is in building the project's identity and raising awareness for cybersecurity issues as a way to pave the way ensure a solid base for the second strategic axis.

- COMPACT Participation - **Engage LPAs/SMEs and IT services providers to cooperate with the project**

The second axis of the plan focuses on engaging LPAs and SME as well as IT services providers to participate in the project development. Participation can take place in two forms: through COMPACT's information hub and by attraction of external COTS providers. Efforts will be made to promote information sharing towards COMPACT's development and to disseminate achieved results. The focus will be on the technological developments once COMPACT Architecture is defined (M13 – May 2018) and COMPACT Platform starts to be developed, validated and demonstrated, as a way to answer to the cybersecurity issues worked on in the first axis.

- COMPACT Uptake/Advocacy - **Position COMPACT as a channel for IT suppliers to deploy new cybersecurity solutions and for LPAs to deal with complex cyber-threats**

The third and final axis of the communication plan sets the foundations for the work to develop further by WP7 – Exploitation. In this final stage the objective is to ensure the platform's future and sustainability beyond the end of the project. The focus from M25 – May 2019 will be on positioning COMPACT as a channel for IT suppliers to deploy new cybersecurity solutions and for LPAs to deal with complex cyber-threats. At this stage, champions

2.1. Key Audiences

2.1.1. Local PA organisations / SME

As the primary end-user of this project, Local Public Administrations take centre stage in COMPACT. On the one hand, the advent of the Internet has improved LPAs efficiency and new specialised network applications such as e-government have enhanced the quality of services provided to citizens. On the other hand, such advancements and trends have also made LPAs more exposed to cyberattacks as these types of institutions deal with sensitive information, which represents an attractive target for a number of threat actors. LPAs have some level of awareness of the risks they take and appreciate the importance of cybersecurity in guaranteeing productivity and to be trusted by the citizens to whom services are provided.

2.1.2. IT security/solutions providers

Because it is COMPACT's objective that its set of tools and services is able to combine solutions and services from multiple sources as it will provide plugins for COTS solutions from Open Source products, IT providers become an important audience to reach. As this is a group already participant in the cybersecurity sector, COMPACT will target them by enquiring their participation in the development phase of COMPACT solution in order to ensure the interoperability of their solutions, in the context of LPAs.

2.1.3. Research community

COMPACT's ambition is also to lead to great innovation to the area of cybersecurity by further developments in the areas of Real Time Security Monitoring, Security Awareness Training and Information Sharing, Cybersecurity Awareness Training based on Gamification Principles, and Threat Intelligence. Findings in these areas will be made public to the relevant research communities.

2.1.4. Local national communities

Considering that LPAs also handle citizens' personal data, their cyber resilience is a matter of public interest and therefore, local citizens are an important group to consider when it comes to informing about the project's development as well as to raise awareness to cybersecurity issues.

According to Eurobarometer 460 [2], there is a generally positive attitude towards the impact of new digital technologies on society, economy and people's quality of life. The majority of the survey's respondents feel confident about their skills to make the most of the opportunities these technologies bring, including when it comes to interact with online public services. Nevertheless, cybersecurity concerns arise and the majority of Internet users have taken actions to deal with online privacy and security issues. These actions range from anti-virus software installation, or change, and being more cautious about sharing personal information or opening emails, to using only their own computers. Although aware of security and privacy features when buying products or using services, not everybody is willing to pay extra for them.

2.2. Key messages per audiences

Table 2 – Messages per Audience

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

2.3. Contribution of Communication and Dissemination to the KPIs of the project

Communication objectives are defined as to allow for close and clear monitoring and in order to properly measure and evaluate the contribution of the Communication and Dissemination actions to the project's overall success.

Table 3 – Communication and Dissemination objectives

	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	>=30	M20-M30

3. Communication and Dissemination actions

Actions can be divided according to the audience they intend to reach directly. A table with potential opportunities for the entire duration of the project will be constantly updated by the project's partners. The document is available to project partners in CyberConnector, and a list already identified of possible events can be found in APPENDIX B.

COMPACT may also participate in the European Commission's Common Dissemination Booster through the integration of a cluster of projects with a common portfolio of results in order to best disseminate them to end-users and to identify exploitation opportunities.

As defined by the EU Guide to Science Communication [3] within the scope of H2020, Communication and Dissemination are at different levels. Therefore, **dissemination actions** are aimed at informing about the project's results to those who may use it in the future, i.e., the research communities. In order to reach this specific audience COMPACT will carry out a number activities described below.

3.1. Scientific publications

COMPACT partners will produce and submit papers on the project's development and results. The papers will be submitted to relevant journals identified during the project. Some relevant publications have already been identified for possible submission:

- International Journal of Human-Computer Studies
- Computers and Society
- Computer Law & Security Review
- IEEE Security and Privacy
- IEEE Transactions on Information Forensics and Security
- International Journal of Information Security
- Information and Computer Security

3.2. Conference presentations

COMPACT partners will present the project's development and results at scientific conferences. The following is a list of relevant conferences that have been identified where the output from COMPACT's activities and development can be presented:

- International Conference on Persuasive Technology
- International Conference on Human Factors in computing Systems
- Symposium on Usable Privacy and Security
- USENIX Security Symposium
- IEEE International Conference on Computer Communications
- International Conference on Computers, Privacy & Data Protection
- NordiCHI Conference
- Cyber Security Romania

In order to reach a wider audience, targeting specific audience benefiting from the project and society, COMPACT will design and implement several **communication actions.**

3.3. Workshops

There are two major workshops scheduled: one in the first year of the project and one in the last year. The first workshop will be limited to a selected number of relevant stakeholders and the second will include a broader audience. Throughout the project partners will identify relevant workshop opportunities in which to take part to present and promote COMPACT, its results and expected impact.

3.4. LPAs / SMEs events

Considering the end-users of the project, COMPACT will target Public Administrations' and Small and Medium Enterprises' events in order to present COMPACT solutions according to the specific needs of these organisations focusing on cybersecurity resilience, and usability and automation as key factors for easy and cost effective deployment and adoption.

3.5. IT industry fairs

Taking into account that COMPACT's integrated platform will be interoperable with major COTS solutions it will be paramount to reach IT and IT security providers with the purpose of presenting the technological solution.

3.6. Targeted meetings

At a more developed stage of the project, targeted meetings will be held both with LPAs/SMES and IT providers in order to present COMPACT solution and secure basis for successful uptake and advocacy of COMPACT and its exploitation, as well as of its components, beyond the project conclusion.

3.7. Contacts with related projects

COMPACT will contact other relevant projects for possible collaboration, cooperation, and cross-fertilization in order to maximise the project's outreach and presentation of results. Throughout the project development, COMPACT aims to contact a minimum of 10 related projects and establish some cooperation with at least 5. Some projects were already identified to be contacted by the partners in order to identify opportunities of collaboration. These projects are listed in the table below.

Table 4 – Related projects to contact

Project Name	Project Website	From	To	Partner
WISER Wide-Impact cyber SEcurity Risk framework	https://www.cyberwiser.eu/	01/06/2016	30/11/2017	ENG
MUSA MUlti-cloud Secure Applications	http://www.musa-project.eu/	01/01/2015	31/12/2017	CINI
CLARUSecure A Framework for User Centred Privacy and Security in the Cloud	http://www.clarussecure.eu/	01/01/2015	31/12/2017	KUL
PaaSword A Holistic Data Privacy and Security by Design Platform-as-a-Service Framework Introducing Distributed Encrypted Persistence in Cloud-based Applications	https://www.paasword.eu/	01/01/2015	31/12/2017	CINI
DOGANA Advanced Social Engineering and Vulnerability Assessment Framework	https://www.dogana-project.eu/	01/09/2015	31/08/2018	ENG

CIPSEC Enhancing Critical Infrastructure Protection with innovative SECurity framework	http://www.cipsec.eu/	01/05/2016	30/04/2019	CINI
HERMENEUT Enterprises intangible Risks Management via Economic models based on simulatioN of modErn cyber-aTtacks	http://cordis.europa.eu/project/rcn/210209_en.html	01/05/2017	30/04/2019	ENG
KONFIDO Secure and Trusted Paradigm for Interoperable eHealth Services	http://www.konfido-project.eu/konfido/	01/11/2016	31/10/2019	CINI

3.8. Media Relations

Relations with the media are very relevant at an early stage of the project in order to ensure COMPACT is associated to the topic of cybersecurity for LPAs. Cybersecurity and its sensationalism brought about by the increase of high-impact attacks which affect society as whole, is a trendy and newsworthy domain. Therefore, it is expected that the media will be open to receiving information on this issue.
Considering that October is European Cyber Security Month, COMPACT took advantage of this timing to officially present the project to the media. In order to do so, a Background Information Kit was developed (Press Release, Brochure, and infographics) to send to targeted media, including both generalist media, which focus on technology and society, and specialised media.
COMPACT project partners have been asked to identify both generalist and specialised media to reach in their respective countries.

3.8.1. Press Releases

At least 7 joint press releases will be issued to the media. Press releases will be produced in English and translated by partners to be sent out to national mass media previously identified. Joint press releases are scheduled according to the project's milestones:

- PR1 – October 2017 (after the second consortium meeting)
- PR2 – November 2017
- PR3 – May 2018
- PR4 – November 2018
- PR5 – May 2019

- PR6 – August 2019
- PR7 – November 2019 (conclusion and evaluation)

Significant achievements and news worthy events may also trigger the issuing of other joint press releases. Besides joint press releases, Partners are also allowed to issue individual press releases mentioning COMPACT. At any moment, partners may also suggest sending other press releases.

At the time of this writing, COMPACT project has issued one joint press release and published it in CORDIS (https://cordis.europa.eu/news/rcn/141757_en.html).

3.8.2. Articles / Interviews

Following upon press releases, efforts will be made to secure positive media coverage on COMPACT in the form of articles, interviews, or journalistic reporting depending on the media and journalists' interests. These efforts are to be developed at a national level by the partners and the project representatives at the Member-State.
Throughout the project partners will pitch the media for the publication of opinion articles on cybersecurity issues promoting COMPACT's potential and capabilities. These articles on specific subject according to the media agenda, may be produced jointly and translated/adapted for national pitching or may be suggested individually by partners.

3.9. Best Practices and Guidelines

From M13 – May 2018 the focus will be on collecting and refining input from gathering success stories, best practices from the national and international expert and end-user groups. The Best Practices and Guidelines will be collected and reviewed during the project, in close link to the Information Hub, in order to make COMPACT easily understandable and quickly adoptable by LPAs

4. Communication Instruments

4.1. Project Logo

In order to ensure and maximise COMPACT's visibility a project's graphic identity is required for visual recognition. A project logo was developed and served as foundation for the website design and development (Deliverable 6.1.) as well as for leaflets, factsheets, brochures, newsletters, presentations, internal project documentation and any other materials that may be needed. The project logo is part of Deliverable 6.1. and full information on its development and usage may be accessed from its accompanying report [4].

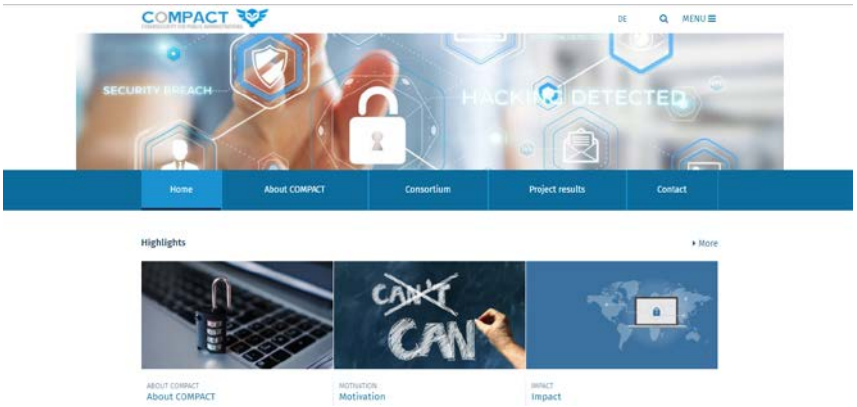
Figure 1 – COMPACT logo with signature

Figure 2 – COMPACT logo

4.2. Project Website

The project website was developed as a key means of communication throughout the project, to be updated with latest news and developments about COMPACT. The project website is part of Deliverable 6.1. and full information on its development, main features, and strategies for efficient implementation may be accessed in its accompanying report [4].

Figure 3 – COMPACT Website - Homepage



4.3. Information Hub

The information hub will be a very important support instrument to gather and share information among LPAs in order to contribute to the development of COMPACT's solution. This hub will be based initially on the CC and LPAs, as well as IT providers, will be asked to join and participate. Later, within the project, the Information Hub may be implemented as a separate Web-based portal similar to those developed by the Health Information Trust Alliance (HITRUST) and the Financial Services-Information Sharing and Analysis Center (FS-ISAC) for the health and financial sectors respectively. The final format of the Information Hub will be defined in the related deliverables, specifically: *D2.4 LPAs Community Model*, *D3.1 Services and Contents Specifications* and *D3.2 Overall COMPACT architecture*, based on the consultation with the LPAs and other relevant stakeholders.

4.4. Promotional materials

In order to support actions implemented during the project, some materials were identified as necessary. At this point, the project has an official PowerPoint presentation, a project brochure, a template for a newsletter, as well as a template to be used by partners when presenting COMPACT. Some infographics have also been developed to support the project communication specially towards the media.

4.4.1. Project Presentation and Presentation template

An official project presentation was produced for partners to use when presenting COMPACT. A presentation template was also produced for partners to use when developing presentations according to specific objectives.

4.4.2. Brochure

A project brochure was developed as a support material to use when presenting COMPACT. The brochure is available in digital file that can be used for online communication as well as a printable format for partners to use as handouts according to their needs when presenting COMPACT at events.

4.4.3. Newsletter

A newsletter template was developed to be used during COMPACT project. A news issue will be released every six months to inform relevant audience on the project status and its news and developments:

- Newsletter no. 1 – May / October 2017
- Newsletter no. 2 – November 2017 / April 2018
- Newsletter no. 3 – May / October 2018
- Newsletter no. 4 – November 2018 / April 2019
- Newsletter no. 5 – May / October 2019

Partners are asked to identify contacts to reach with newsletters thus creating audience-specific contact lists (LPAs, SMEs, IT providers, research communities, and others entities relevant to the project).

4.4.4. Infographics and Factsheets

Two infographics were developed to support communication actions. The focus of these first infographics is on general cybersecurity issues in the context of LPAs, *i. e.*, the main challenges these organisations face, the main threats COMPACT focuses on, and the expected impact of COMPACT (ANNEX B). Other infographics may be developed as the project progresses and gets more results in order to support the project's communication with visual materials.

4.5. Social networks

Social media are currently the main means used by people to keep up to date with the daily news. COMPACT recognizes the important of social media and four social networks accounts were created to provide updates about the project and communication channels for different types of audience. The contents and messages published on each different social network is curated to reflect the type of audience associated to the specific social network. In addition to its own content, COMPACT should share content from other sources that align with the project's objectives.

Partners are being asked to identify and share information they consider to be relevant for the project. There has been a weekly rotation schedule to ensure that the project has a dynamic presence in social networks – one partner per week has to suggest content. They should also share COMPACT content and identify COMPACT by using its social networks handles. Social media accounts are managed by the WP6 leader who collects the contributions of partners and publishes the content according to their fit to each social network. The WP leader also monitors the performance of publications through social media analytics.

4.5.1. Facebook

@COMPACTproject
In addition to project news and results, content on Facebook should focus on messages to a wider, non-specialised audience, with advice and rules to raise awareness for safer behaviour while online. Content should be sharable – short and creative copy using mostly images and short videos to engage audiences. Also, COMPACT will share news on cybersecurity issues.

4.5.2. Twitter

@COMPACTproject
Twitter is being used mostly to inform on project results and news as well as connecting to other relevant projects and European institutions engaging (liking, retweeting, commenting) with other relevant accounts cybersecurity.

4.5.3. LinkedIn

https://www.linkedin.com/company/22295613/
Content for LinkedIn focuses on project news and results, aiming especially to inform on technological developments. As it is a professional network, LinkedIn is a privileged channel to reach the IT industry as users tend to interact by showcasing the benefits of COMPACT for business development.

4.5.4. YouTube channel

https://www.youtube.com/channel/UCTiDsa1dVYs7sXDtz0LtcDA
YouTube channel will serve as a platform for video content about COMPACT. Videos of consortium meetings and workshops may be produced to promote COMPACT's

development and technology and feed the channel. Animated short videos may be considered to promote the project's findings. Videos should always be shared in other social networks to reach wider audiences.

4.6. Videos

Two videos will be produced throughout the project. A first video presenting COMPACT is under production and a second one will be produced towards the end of the project focusing on COMPACT's results.

4.7. Blogs

COMPACT will take a proactive approach, through its partners, to actively participate in blogs identified as relevant for the project's visibility and promotion.

Table 5 – Overview Target Audience / Messages / Actions / Instruments

Target Audience	Messages	Actions	Instruments
LPAs / SMEs	• Cybersecurity issues affecting organisations • Learning through gamification • Knowledge sharing – information hub • COMPACT's usability and automation	• Sending of presentation kit • Workshops • Events • Meetings	• Promotional materials • COMPACT website • Information Hub (CC) • Social networks • Blogs
IT security / solutions providers	• "Cloud-enabled" and "Cloud-ready" solution • COMPACT's usability and automation • Technology Readiness Level	• Industry fairs • Targeted meetings • Media relations (specialised media)	• Promotional materials • Press release • Articles/Interviews • Social networks • Blogs
Research community	• Technology Readiness Level • Learning through gamification	• Scientific publications • Conference presentations	• Papers • Promotional materials • Blogs
Local national communities	• Cybersecurity risks in everyday behaviour	• Media relations (generalist and specialised media media)	• Background Information Kit • Press release • Articles/Interviews • Social media

5. Contribution of partners to communication and dissemination

The implementation of this plan is to be accomplished by multiple partners of the consortium acting cooperatively. But it is also complemented by individual activities by the partners in order to enhance and maximise COMPACT's outreach.

Table 6 – Individual contribution of partners

Partner	Actions
ENG	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.
CINI	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 internally disseminate COMPACT results 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 plans to participate in local workshops with public and potential end users for communication of project results and will use its regional innovation network for project information promotion. Additionally, a wide direct dissemination, via meetings, will be carried out in Portugal encouraging an active dialogue with local authorities to facilitate the fast adoption of the project results by local end users.
SIL	SIL consultants participate at and co-organize a number of information security conferences and events around the world. The primary channels through which Silensec will disseminate the results achieved through COMPACT will be: Cyberdrills and cyber security events organized by the International Telecommunication Union (ITU) around the world for National CERTs and

	Governments; private security conferences including but not limited to "Cyber Security Romania", RSA Europe; Publication in international journals.
S21sec	S21sec will disseminate the project results to their customers and network contacts through its marketing channels: website, social network profiles, publications, etc. together to the organisation of conferences and workshops.
ISCOM	ISCOM will communicate and disseminate COMPACT results to other national CERTs - such as: the Spanish one (INCIBE), the Romanian one (CERT.RO), and more - as well as to Italian SMEs and citizens, also via the organization of public events.
AIT	The dissemination of results by AIT will be realized by multiple paths to address a broad audience and a wide range of stakeholders. Dissemination on a scientific level will be done by publicizing at international recognized conferences and in scientific journals.
KUL	The results from the work performed under COMPACT will be disseminated mainly towards the broader society by academic publications in scientific journals and by participating in high-level workshops and/or conferences. Papers will be submitted and a panel will be organised at industrial and academic conferences. Legal technical and scientific articles will be submitted for publishing in relevant peer-reviewed journals.
KSP	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	CMA will ensure the dissemination of results by promoting information sessions / workshops, directed initially to users within the municipal services, connected to the internal network. It is intended to extend these information sessions / workshops to all municipal employees, including those who are to serve in primary schools of the 1st cycle and kindergartens. It also seeks to make use of internal and external tools that enable the dissemination of information (intranet and municipal internet, press review, municipal bulletin)
CDA	CDA will promote meetings, workshops and ICT based advices in order to bring the results of COMPACT inside and outside the Municipality. There will be 5 use cases, based on audience type: i) Municipality Managers - Specific meetings, in collaboration with the ICT department Engineers with the objective of gaining security awareness by creating new security-in-mind working policies and ideas for security promoting. ii) Municipality ICT technicians - training on site for right implementation of software and policies inside the ICT structure; iii) Municipality Workers - eLearning events/workshops about information and data security, related to their activities and the possible threats. Training and explanation of new security procedures; iv) Students - School meetings for security awareness; v) Citizens - Specially designed Afragola's Website section and public advices will aware citizens about possible threats and new security policies applied.
BOL	BOL will disseminate results by promoting public events, information sessions / workshops. BOL will also use internal and external tools that enable the

	dissemination of information like intranet and municipal internet, press review and social media presence.
DSS	DSS will disseminate the project information and results through its public channels (website, social networks, etc.). Besides this, conferences, publications and internal and external workshops are also planned.
BIT	BIT will disseminate the tools (gamification) internally in the magistrate to make the employees aware of said tools. A campaign is planned where incentives for using the games and awareness assessment tools are offered. Through the magistrate the project can be disseminated in networks of the public administrations, where Bremerhaven is a member.

6. Monitoring and Evaluation

Communication and Dissemination actions will be monitored using the following approach:

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

Table 7 – Communication evaluation

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 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 communication and dissemination

All partners are asked to participate in identifying dissemination and communication opportunities. To this purpose, there is an Input and Monitoring document available in CC where partners can, not only register opportunities for promoting COMPACT, but also monitor their activities and share them with the consortium. This document should be updated monthly in order to contribute to Communication and Dissemination Plans and Reports.
In addition to this, activities should be communicated as soon as possible to the WP leader with a short summary so as to contribute to feed the project website and social networks on COMPACT's activities. Whenever possible, partners should add photos and/or videos of the activities developed – conference presentations, workshops, industry events, etc.

8. Conclusions

Considering COMPACT's overarching objective of enabling LPAs to become the main actors of their own cyber-resilience improving process by providing them with effective tools and services for removing security bottlenecks, 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.
In order to do so, COMPACT has designed a strategy based on strategic axes – **Outreach/Awareness, Participation, and Uptake/Advocacy** to be motivated as the project develops and comprising several target audiences, through direct and indirect communication actions, in response to the stated communication and Dissemination objectives. Through collaboration between the consortium, as well as through individual initiatives, the defined strategy aims to **build and maintain relationships with LPAs and IT providers** in order to develop the best possible technological solution that truly responds do LPAs needs, to **further research in cybersecurity**, and to promote professional connections with external stakeholders that may **support COMPACT's exploitation and success** beyond the conclusion of the project.
This version of the deliverable focuses mainly on the first axis of the strategy – Outreach/Awareness. There are planned two other versions of the Communication and Dissemination Plan that will build on this one as the projects develops.

9. References

[1] COMPACT Description of Action (DoA)

[2] Special Eurobarometer 460: Attitudes towards the impact of digitalisation and automation in daily life. Directorate-General for Communication, 2017. Available at

http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/78998

[3] The EU Guide to Science Communication. EU Science & Innovation, 2016. Available at https://www.youtube.com/playlist?list=PLvpwIjZTs-Lhe0wu6uy8gr7JFfmv8EZuH

[4] COMPACT Deliverable 6.1 – Project Website and Logo

10. APPENDIX A – CHRONOGRAM OF ACTIONS [M1-M15]

Actions	Start	Finish	Partner(s)	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15
				may/17	jun/17	jul/17	aug/17	sep/17	oct/17	nov/17	dec/17	jan/18	feb/18	mar/18	apr/18	may/18	jun/18	jul/18
Talk at 13th TAROT Summer School on Software Testing, Verification & Validation	Mon 26/06/17	Fri 30/06/17	CINI															
Talk at The Axis Way - Smart Innovation Lab	Thu 21/09/17	Thu 21/09/17	CINI															
COMPACT Press Release 1	Fri 06/10/17	Fri 06/10/17	Consortium															
Presentation at Cyber themes from CNCS - Cybersecurity in the Workplace	Mon 16/10/17	Mon 16/10/17	CMA															
Presentation at ViR-Nordwet Plenum 2017	Wed 25/10/17	Thu 26/10/17	BIT															
COMPACT Newsletter 1	Tue 31/10/17	Tue 31/10/17	Consortium															
Workshop Takedown Project	Wed 16/11/17	Wed 16/11/17	KUL															
Presentation at VITAKO	Thu 23/11/17	Sun 26/11/17	BIT															
COMPACT Press Release 2	Thu 30/11/17	Thu 30/11/17	Consortium															
COMPACT Workshop	Thu 18/01/18	Thu 18/01/18	INOV															
International Conference on Persuasive Technology	Mon 16/04/18	Thu 19/04/18	AIT															
International Conference on Human Factors in computing Systems (CHI)	Sat 21/04/18	Thu 26/04/18	AIT															
COMPACT Newsletter 2	Mon 30/04/18	Mon 30/04/18	Consortium															
COMPACT Press Release 3	Thu 31/05/18	Thu 31/05/18	Consortium															
COMPACT Social networks update	Tue 01/08/17	Tue 31/07/18	Consortium															
COMPACT Website update	Wed 23/08/17	Tue 31/07/18	Consortium															
Major Cities of Europe Conference	TBD	TBD	BIT															
Internal webinars	TBD	TBD	ENG															

11. APPENDIX B – LIST OF POSSIBLE EVENTS

Event	Type of Event	Audience	Date	Location	Contact	Obs.
15th International Conference on Applied Cryptography and Network Security (ACNS)	Conference	Academia and industry	Jul 10-12	Kanazawa (Japan)	https://cy2sec.comm.eng.osaka-u.ac.jp/acns2017/index.html	Registration: June 28
26th USENIX Security Symposium	Symposium	Researchers, practitioners, system administrators and programmers	Aug 16-18	Vancouver, BC (Canada)	https://www.usenix.org/conference/usenixsecurity17	Workshops: August 14-15 Registration: July 24
30th IEEE Computer Security Foundations Symposium (CSF)	Symposium	Researchers	Aug 21-25	Santa Barbara (USA)	http://csf2017.tecnico.ulisboa.pt/index.html	Workshops: Aug 21
22nd European Symposium on Research in Computer Security (ESORICS)	Symposium	Researchers	Sep 11-13	Oslo (Norway)	https://www.ntnu.edu/esorics2017	Workshops: Sepetember 14-15 Registration: August 16
20th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)	Symposium	Academia, government, and industry	Sep 18-20	Atlanta, Georgia (USA)	https://www.raid2017.org/	
LASER - Learning from Authoritative Security Experiment Results	Workshop	Researchers	Oct 18-19	Arlington (USA)	http://2017.laser-workshop.org/	Deadline for Papers: July 15
24th ACM Conference on Computer and Communications Security (CCS)	Conference	Researchers, practitioners, developers, and users	Oct 30 - Nov 3	Dallas, Texas (USA)	https://www.sigsac.org/ccs/CCS2017/venue.html	Workshops: October 30 and November 3 Deadline for Tutorials: July 3

3rd Annual Public Sector Transformation Conference	Conference	Public Administration	Nov 7 (2017)	Brussels (Belgium)	http://www.eu-ems.com/summary.asp?event_id=4339&page_id=9261	**"Connecting the Citizen: Realising the Potential of Smart Cities"** For more information on sponsorship or exhibiting please download the sponsorship brochure here or contact Rose Maloney at digitalpublic@forum-europe.com or on +44 (0) 2920 783 070.
ITAPA 2017 International Congress	Congress	Public Administration	Nov 14-15 (2017)	Bratislava (Slovakia)	http://www.itapa.sk/itapa-congress/	Information Technologies and Public Administration
ADV-Tagung Verwaltungsinformatik 2017	Conference	Public Administration	Nov 16 (2017)	Vienna (Austria)	https://www.adv.at/Events/Event-Items/ADV-Tagung-Verwaltungsinformatik-2017	**"Digitalisation in the Public Sector - Science and Business Dialogue"** Lecturers, sponsors, products and knowledge are welcome! Contact michaela.brank@adv.at Tel.: +43 1 5330913-71 Handy: +43 699 15330971

5th Annual European Cybersecurity Conference	Conference		Nov 23 (2017)	Brussels (Belgium)	http://eu-ems.com/summary.asp?event_id=4337&page_id=9242	To discuss any speaking, sponsorship or visibility opportunities please contact Anne-Lise Simon on +44 (0) 2920 783 023 / anne-lise.simon@forum-europe.com
33th Annual Computer Security Applications Conference (ACSAC)	Conference	Academia, Industry, Government	Dec 4-8 (2017)	San Juan, Puerto Rico (USA)	https://www.acsac.org/	Deadline for Works in Progress: September 8 Registration: September (begins)
13th International Conference on Information Security Practice and Experience (ISPEC)	Conference	Researchers and practitioners	Dec 13-15 (2017)	Melbourne (Australia)	http://nsclab.org/ispec2017/	Deadline for Papers: Aug 5
13th International Conference on Persuasive Technology	Conference	Researchers and practitioners from industry and academia	Apr 16-19 (2018)	University of Waterloo (Canada)	http://www.persuasive2018.org/	**Important dates** Submission deadline: **November 1, 2017** Decision notification: **January 15, 2018** Camera ready version: **January 31, 2018**
International Conference on Human Factors in computing Systems (CHI)	Conference	Researchers and practitioners	Apr 21-26 (2018)	Montreal (Canada)	https://chi2018.acm.org/	Deadline for Papers: September 12
39th IEEE Symposium on Security and Privacy (S&P)	Symposium	Researchers and practitioners	May 21-23 (2018)	San Francisco, CA (USA)	https://www.ieee-security.org/TC/SP2018/	Deadline for Papers: Ongoing (1st of each month)

20th International Conference on Computational Intelligence in Security Information Systems (ICCISIS)	Conference	Academic scientists, researchers and research scholars	Jun 11-12 (2018)	Copenhagen (Denmark)	https://www.waset.org/conference/2018/06/copenhagen/ICCISIS	**Important Dates** **Oct 20**, 2017 - Abstracts/Full-Text Paper Submission Deadline **Oct 31**, 2017 - Notification of Acceptance/Rejection **Feb 11**, 2018 - Final Paper (Camera Ready) Submission & Early Bird Registration Deadline
16th International Conference on Applied Cryptography and Network Security (ACNS)	Conference	Academia and industry	Jul 3-5 (2018)	Leuven (Belgium)	https://www.cosic.esat.kuleuven.be/events/acns2018/	**Important dates** **Jan 26**, 2018 – Submission deadline **March 31**, 2018 – Notification deadline **May 25**, 2018 – Early registration
7th International Conference on Cloud Computing and eGovernance 2018	Conference		Jul 23-24 (2018)	University of Greenwich (UK)	http://iccceg.org/	**Important dates** **Jun 30**, 2018 - Paper Submission Acceptance Notification Continuous Process **Jul 08**, 2018 - Author Registration **Jul 08**, 2018 - CRC & Copyright Submission **Jul 15**, 2018 - Listener Registration

14th Symposium on Usable Privacy and Security	Symposium	Academia and industry	Aug 12-14 (2018)	Baltimore, MD (USA)	https://www.usenix.org/conference/soups2018	**Important dates** Abstract submissions due: Monday, February 12, 2018 Full paper submissions due: Friday, February 16, 2018
27th USENIX Security Symposium	Symposium	Researchers, practitioners, system administrators and programmers	Aug 15-17 (2018)	Baltimore, MD (USA)	https://www.usenix.org/conference/usenixsecurity18	The Call for Papers will be available in Fall 2017.
IEEE International Conference on Computer Communications	Conference	Research Community	Apr 15-19 (2018)	Honolulu, HI (USA)	http://infocom2018.ieee-infocom.org/	
11th International Conference on Computers, Privacy & Data Protection	Conference	Academics, lawyers, practitioners, policy-makers, industry and civil society	Jan 24-26 (2018)	Brussels (Belgium)	http://www.cpdpconferences.org/	
22nd European Symposium on Research in Computer Security (ESORICS)	Symposium	Researchers	Sep -- (2018)	--	-	
10th NordiCHI Conference	Conference		Oct 1-3 (2018)	Oslo (Norway)	http://www.nordichi2018.org/	**Important dates** Submission deadline: 15 April 2018
31st IEEE Computer Security Foundations Symposium (CSF)	Symposium	Researchers	TDB	TDB	-	
Cyber Security Romania	Congress	State, Academia, Private Companies, Specialists	TBD	Romania	https://cybersecurity-romania.ro/	