



Project Title	Wide – Impact cyber Security Risk framework
Project Acronym	WISER
Grant Agreement No	653321
Instrument	Innovation Action
Thematic Priority	Cybersecurity, Privacy & Trust, Risk Management, Assurance Models
Start Date of Project	01.06.2015
Duration of Project	30 Months
Project Website	www.cyberwiser.eu

D8.6 COMMUNICATION PLAN FINAL VERSION

Work Package	WP8, Go to market
Lead Author (Org)	Stephanie Parker (Trust-IT)
Contributing Author(s) (Org)	Paolo Lombardi, Niccolò Zazzeri, Timea Biro (Trust-IT); Atle Refsdal (SINTEF), Ales Cernivec (XLAB), Antonio Álvarez (ATOS)
Due Date	31.05.2017
Date	26.06.2017
Version	1.0

Dissemination Level

<input checked="" type="checkbox"/>	PU: Public
<input type="checkbox"/>	PP: Restricted to other programme participants (including the Commission)
<input type="checkbox"/>	RE: Restricted to a group specified by the consortium (including the Commission)
<input type="checkbox"/>	CO: Confidential, only for members of the consortium (including the Commission)



Versioning and contribution history

Version	Date	Author	Notes
0.1	03.05.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri Trust-IT (Trust-IT)	ToC and al location of sections
0.2	08.05.2017	Atle Refsdal (SINTEF)	First internal review
0.3	09.05.2017	Ales Cernivec (XLAB)	First internal review
0.4	17.05.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri Trust-IT (Partner 2)	Answers to First internal review
0.5	22.05.2017	Atle Refsdal (SINTEF)	Second internal review
0.6	15.06.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri Trust-IT (Trust-IT)	Response to second internal review and harmonization with D2.6 and D8.3
0.7	16.6.2017	Aleš Černivec (XLAB)	Second internal review
0.8	16.6.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri Trust-IT (Trust-IT)	Response to second internal review and refinement of Executive Summary
0.9	22.06.2017	Stephanie Parker, Paolo Lombardi, Niccolò Zazzeri Trust-IT (Trust-IT)	Add section 4.2
0.10	23.06.2017	Antonio Álvarez (ATOS)	Overall check and submission to GA for approval
1.0	26.06.2017	Antonio Álvarez (ATOS)	Submission to EC

Disclaimer

This document contains information which is proprietary to the WISER Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to a third party, in whole or parts, except with the prior consent of the WISER Consortium.

Table of Contents

Versioning and contribution history	ii
Executive Summary	5
1 Introduction	6
1.1 WISER Communication Strategy	6
1.2 Goals	7
1.3 KPIs	8
1.4 Overall KPIs status and mitigation actions	12
1.5 Community Database	12
1.6 A Joint Effort	13
1.7 A Living Document.....	13
2 WISER Package Offers and Markets.....	13
2.1 WISER Cyber Risk Monitoring Services.....	13
2.2 WISER Cyber Risk Awareness Free Services	15
2.3 WISER Markets and Target Audiences.....	16
3 Year Two Achievements: Multi-channel and Multi-stakeholder Engagement.....	17
3.1 Media Platform and Content Creation	17
3.2 Social Media Networks	20
3.3 Events.....	24
3.4 Media Visibility and Publications	26
3.4.1 CyberWISER Essential & Plus Launch Campaign.....	26
3.4.2 Articles and Publications	27
4 Communication Plan for last six months of WISER.....	28
4.1 Strategic goals for 6-month WISER sprint.....	28
4.2 Support of Portability to Verticals	28
4.3 Formats and Channels	29
4.4 WISER Event Planner	30
4.4.1 WISER Final Event.....	30
4.5 Market Target 1 – Small Firms	32
4.5.1 Strategy and Expected Impact	32
4.5.2 Messages, Channels and Formats	33
4.5.3 Actions and Targets for Small Firms – Last six months.....	36
4.6 Target Market 2 – Large Companies.....	37
4.6.1 Strategy and Expected Impact	37
4.6.2 Messages, Channels and Formats	37
4.6.3 Actions and Targets for Large companies – Last six months	40
4.7 Target Market 3 – Public Sector.....	41
4.7.1 Strategy and Expected Impact	41
4.7.2 Messages, Channels and Formats	41
4.7.3 Actions and Targets for Public Sector – Last six months.....	43
4.8 Market Target 4 – Policy Stakeholders in EU and Internationally	44
4.8.1 Strategy and Expected Impact	44
4.8.2 Messages, Formats and Channels.....	45
4.8.3 Actions and Targets for Policy & Standard Bodies – Last six months	47
4.9 Market Target 5 – General Public.....	48
4.9.1 Strategy and Expected Impact	48
4.9.2 Messages, Formats and Channels.....	48
5 Last six months Roadmap (June 2017 – November 2017)	49
6 Conclusions	49
7 Annex 1 – Complete List of Media Channels Targeted.....	51

8 Annex 2 Sample of communication material55

List of Tables

Table 1 - WP8 - KPI8.1: Web and social outcomes.....	10
Table 2 - WP8 - KPI8.2: Target market outreach & stakeholder response	11
Table 3 - WP8 - KPI8.2: Target market outreach & stakeholder response	11
Table 4 - WP8 - KPI8.4: Market prospects, leads generated & commercial agreements	11
Table 5 - KPIs for Target Audiences	17
Table 6 - Sample of Content Creation in Year Two	20
Table 7 - WP8 - KPI8.2: Target market outreach & stakeholder response	21
Table 8 - Targeted Tweet Examples	24
Table 9 – WISER Event Presence.....	25
Table 10 - Contacts for the CyberWISER Essential & Plus campaign	26
Table 11 - Formats for Year Two	30
Table 12 - WISER Event Planner for last six months	32
Table 13 - Updated Formats for engaging Small firms	35
Table 14 - Updated sample of channels for reaching small firms	35
Table 15 - Actions and Targets for Small Firms.....	36
Table 16 - Updated Formats for engaging Large Companies	38
Table 17 - Updated Channels for targeting Large Companies	39
Table 18 - Actions and Targets for Large companies	40
Table 19 – Updated Formats for engaging the Public Sector.....	42
Table 20 - Updated Channels for engaging the Public Sector.....	42
Table 21 - Actions and Targets for Public Sector	43
Table 22 – Updated Formats for engaging with Policy Stakeholders	45
Table 23 - Updated Channels for reaching Policy Stakeholders	46
Table 24 - Actions and Targets for Policy & Standard Bodies	47
Table 25 - Channels and Formats for engaging with General Public	48
Table 26 - Last six months Roadmap	49

List of Figures

Figure 1 - Flash Report example	7
Figure 2 - Branding of CyberWISER product packages	13
Figure 3 - The WISER 3-level offer (CyberWISER Light, Essential, Plus)	15
Figure 4 - WISER Cartography & Socio Economic Impact Tool.....	15
Figure 5 - Essential Guide to the NIS Directive	18
Figure 6 - www.cyberwiser.eu.....	19
Figure 7 - Example of messages in national language	22
Figure 8 - Visibility and Impact on Social Media	23
Figure 9 - WISER Final Event first draft agenda.....	31

Executive Summary

WISER is an innovation action and, as such, it puts considerable effort into defining a sustainable go-to-market path. *Work Package 8 – Go to Market* plays a fundamental role in defining the what, who, when and how, but can only go so far in delivering key goals. For this reason, we are delivering this updated plan, with the full commitment of partners in acting upon the actions defined.

This document is the final version of the Communication Plan, covering the actions and impact for the period May 2016 to May 2017 and the plans for the last 6 months of the project (June-November 2017) as part of an all-partner commitment to communicating WISER and disseminating its results to the diverse audiences targeted.

This plan is now the focus of WP8 based on three pillars namely a complete product range for major marketing campaigns, portability to other verticals for verification (Manufacturing, Transportation, ICT, Healthcare and connected devices, Public Administrations) in addition to a wide pool of SMEs that also but not only operate in these verticals and a business model to be tested.

The overriding strategic objective is to boost the use of CyberWISER service packages by focusing activities around SMEs and verticals. Specifically, WISER seeks to achieve KPIs related to the WISER exploitation objectives.

These activities will cover dedicated web sections e.g. targeting verticals and SMEs (new CW-SEIT tool), Media Kits targeting also the verticals identified, a series of stakeholders' events including the WISER final event and social media campaigns based on specific goals and messages, timely and insightful communications.

The outcomes of the plan will be communicated in the final project report.

This document is delivered at the same time (M24) as two other key deliverables 8.3 Practical tools for assessing the socio-economic impact of risk management implementation for cybersecurity, final version; and D2.6 Wiser product strategy, final version.

D8.3 reports on findings from an updated and extended analysis of the cyber risk landscape and presents the final development of CW-SEIT based on the new analysis with direct feedback from the SME community.

D2.6 provides an overview of the product vision of WISER consolidating WISER's market positioning and setting the path to its "go-to-market" strategy. To this end the WISER

The three deliverables (D8.6, D8.3 and D2.6) are complementary and share the same strategic objective: to boost the use of CyberWISER service packages by focusing activities around SMEs and verticals.

A key next step for the WISER project is to align these documents in preparation for D8.8 Exploitation plan and business models, final version (M30).

1 Introduction

1.1 WISER Communication Strategy

The WISER communication activities will follow a **SMART approach** (specific, measurable, achievable, realistic, targeted and timed) for planning and monitoring communications about WISER and dissemination of results.

Specific: WISER targets its communication activities to five main target audiences (Section 2.2). WISER uses a diverse set of formats, channels & specific messages to engage with different target audiences (Section 4.1).

Measurable: actions are related to a pre-defined set of KPIs.

Achievable and realistic: A monthly checklist defines actions in concert with all partners and in line with the communication plan while allowing WISER to react swiftly to new promotional and dissemination opportunities.

Targeted and timed: The checklist ensures actions are timely with clearly defined target audiences.

The key performance indicators (KPIs) ensure a continuous stream of activities around the WISER goals and rollout of tools and services. We align the KPIs with a good understanding of WISER priorities and use them as key factors in evaluating the impact of effort spent on a particular activity. The KPIs also serve as a driver for staying up-to-speed on developments in the cyber risk landscape.

A **monthly checklist** shared with partners describing activities planned on a monthly basis to allow for major developments in the cyber risk landscape.

As a starting point, WISER has identified an internal set of target on core activities and KPIs shared with all partners:

- **Content update on Cyberwiser.eu:** Minimum 8 updates per month
- **Social media Twitter:** Minimum 16 tweets per month
- **Social media LinkedIn:** Minimum 8 updates per month
- **Events:** Minimum 1 every 3 months
- **Press & Media content:** Minimum 1 publication (e.g. PR, industry announcement) every 3 months
- **Newsletters:** Minimum 1 newsletter every 3 months

Monitoring with Flash Reports: The continuous monitoring of the key performance indicators and overall communication and marketing performance is the basis for setting future targets as WISER increasingly approaches market rollout. Each iteration of the plan reports on the progress made and, may, based on project developments and/or new market data, lead to minor adjustments in the KPIs set and the effort dedicated to fit the evolving go-to-market goals. This will reflect the dynamic nature and flexibility of WP8 in adapting its go-to-market strategy, taking on board also the feedback from the Early Assessment Pilots in WP6, as well as the response to the launch of the WISER services.

WISER - Flashreport 01-06-2015/ 30-11-2017												as of: 13 June 2017	
KPI	Target by the end of the project	Target by the end of Year 2	Cumulative as of today	Q2/15	Q3/15	Q4/15	Q1/16	Q2/16	Q3/16	Q4/16	Q1/17	Q2/17 as of today	Q2/17 (Est)
KPI8.1a Unique visitors [#]	600-800/month	300-500/month	12,547	672	1,574	1,007	904	1,977	1,860	1,752	1,575	1,226	1,147
Unique visitors [% QoQ]	5%	5%	-	-	57%	-56%	-11%	54%	-6%	-6%	-11%		
KPI8.1b Page views [#]	1500-3000/month	1000-1500/month	58,029	1,655	4,375	3,889	4,502	8,275	10,619	9,722	8,254	6,738	6,394
KPI8.1c Sessions [#]	700-1000/month	400-700/month	19,994	844	2,039	1,559	1,452	2,981	2,923	3,551	2,544	2,101	2,001
Average session [s]	120	100	-	92	133	160	197	169	272	177	236	215	210
KPI8.1d Content update on Cyberwiser.eu	240	120	144	11	22	23	15	11	8	11	25	18	16
KPI8.1e Newsletters	10	5	6	-	-	-	-	1	1	3	1	0	0
KPI8.1f Press & Media materials	10	5	24	3	0	2	2	3	0	1	9	4	3
KPI8.2a Registered users [#]	1500	750	198	0	4	7	14	76	46	24	13	14	14
KPI8.1b Twitter followers [#]	350	150	310	32	11	30	56	40	43	46	34	18	14
KPI8.1c Tweet Sent [#]	480	240	1447	158	119	107	205	268	202	128	80	30	19
KPI8.1d LinkedIn Connections [#]	500	250	992	0	0	0	80	205	322	230	83	72	70
KPI8.1e LinkedIn Update/Post [#]	240	120	198	-	-	0	12	90	27	39	21	9	6
KPI8.1f Overall Community Database [#]*	2350	1150	1500	32	15	37	150	321	411	300	130	104	98
KPI8.1g EAPs active [#]**	10	10	11	-	10	11	11	11	-	-	-	-	-
KPI8.3a Data collection [#]	50	25	117	15	13	12	15	13	10	15	15	9	8
KPI8.4a Leads generated [#]**	90%		2									2	
KPI8.4b Performed CyberWISER Light Sessions [#]**	1000	500	157										
KPI8.4c Commercial agreements (Basic & OR Advanced Session) [#]**	50	25	1									1	
* Includes Registered Users, Twitter Followers & LinkedIn connections													
** Linked to other WP activities													

Figure 1 - Flash Report example

Already at the start of the project, WISER implemented a process for monitoring the actions taken in year one of the project – Flash Reports (see Figure 1), which are shared with the Consortium on a monthly basis, and used as a basis for quarterly reporting selecting the most relevant indicators, Communication activities developed within WP8 mainly aim at building trust around the WISER tools and services. We achieve this objective by:

- Contributing to a common understanding of cyber risk management best practices aligned with the objectives of the European Cyber Security Strategy and the plan for the Digital Single Market¹.
- Tailoring messages to the different target groups based on their specific levels of knowledge and IT security expertise, thus managing their expectations effectively. Continuous monitoring of the landscape, IT and business media, reports etc. through desk research.
- Establishing synergies with relevant initiatives in Europe and internationally, providing insights on new regulations and policy priorities related to cyber security and the Digital Single Market, and showcasing best practices, drawing on the analysis provided in D6.2 - Best Practices & Early Assessment Pilots, Final Version on applicable standards, security testing and vulnerability monitoring. Communication activities will also draw on Task 6.5 - Synergies and international liaison on best practices.

Another major objective of the communication strategy is to maximise the visibility and awareness of the project, to contribute to the impact creation by communicating and ensuring the target users' understanding of the project concept, results and potential applications. Communication will also play a key role for the business exploitation of WISER results.

1.2 Goals

The WISER communication strategy is aimed at maximising the visibility and awareness of the WISER project, and increasingly market its offer to different customers, based on their specific needs. The communication strategy also contributes to educate communities on cyber security and risk

¹ <http://www.euractiv.com/sections/infosociety/ansip-cybersecurity-public-private-partnership-launch-early-next-year-314448>.

management, including the costs of poor risk assessment and practices. To this end, WISER promotes best practices and creates international alliances around common goals, such as raising awareness about the role of standards in establishing interoperability and global collaborative platforms.

In more details, the main **WISER communication strategy's goals** are:

- To widely communicate the benefits of WISER in a way that educates, informs and builds a trusted relationship over time – delivery of up-to-speed cyber security awareness messages, explaining implications for European industries and businesses.
- To build a WISER community based on Social Media engagement, face to face interactions, event participation. The community developed is the basis to communicate shared knowledge, messages and discussions about Cyber Security and Risk Management while identifying different stakeholder groups. Specifically, WISER is focusing on a community covering the current vertical markets related to its full scale pilots and early assessment pilots, as well as across sectors not currently covered to support WP7.
- To analyse the market and price structure of cyber security and insurance market in order to position WISER and strategically plan stakeholder engagement in pilot verticals, energy and finance, and the SME community. To gain deep understanding of prospective customers, this task will systematically analyse user experience (e.g. business relevance and input for customer journey mapping), in synergy with WP7, based on the current analysis provided in D7.3.
- To educate and raise awareness on Cyber Security key role for today's digital businesses, industries and SMEs, as well as on new EU regulations, such as the Network and Information Security Directive (NISD). This activity thus promotes the work undertaken in WP6 on the national cyber security strategies and supports the EC policy approach to building cyber security capacity across the member states. This aim is to assist organisations affected by regulatory changes in aligning their cyber security strategy with new reporting obligations². In addition to the planned online cartography of national strategies, WISER has implemented a new web section, Policy Guide, offering practical guide and advice on new regulations.
- To present best practices, standards, case studies and practical tools in order to contribute to increase the cyber risk awareness by educating SME decision makers, risk managers and boards of directors across the market. This activity draws on work undertaken in the WISER technical WPs and in WP6, identifying gaps that WISER can help fill, as well as partner contributions to national strategies.

The communication strategy will also contribute to the impact creation by communicating and ensuring the target users understand the project concepts objectives and results.

1.3 KPIs

The impact of the activities performed are measured through a core set of key performance indicators (KPIs) wherever they are quantifiable.

A continuous activity of monitoring will be carried on by Trust-IT and shared with all partners monthly.

Social media activities will include active contributions to specific Social Media such as Twitter, LinkedIn and contributions to discussion groups, direct messaging and leveraging current connections within the consortium with the aim to build a loyal support base.

Thanks to its continuous Social Media presence WISER will be able to identify new topics and trends on cyber security and risk management and to contribute to tackle the key role of these two topics

² Actions are also based on WISER participation in related events, such as the DG CNECT Cloud Security Workshop (18 March 2016), taking on board not only insights from the EC but also challenges around implementation.

through its five market targets. WISER will monitor its social influence and engagement through a set of initial KPIs based both on web platform statistics and Social Media activities and results.

A list of smart and general KPIs to monitor the project progress, as requested by the European Commission, has been produced. Tables 1-4 below show the end of year two and the end of project targets together with the current value of each KPIs. In addition to the monthly Flash Reports, WISER produces a monthly checklist indicating upcoming activities and targets in relation to the End of Project targets.

Name	Definition	Measurement methods	Thresholds	Current Value
KPI8.1a Unique visitors	Number of users that have had at least one session on www.cyberwiser.eu Includes both new and returning users.	Sum-up tracked via Google Analytics	Year 2 target: 300-500/month End of project target: 600-800/month	501
KPI8.1b Page views	Total number of website pages viewed.	Sum-up tracked via Google Analytics	Year 2 target: 1000-1500/month End of project target: 1500-3000/month	2321
KPI8.1c Sessions	Total number of Sessions registered on www.cyberwiser.eu . A session is the period time a user is actively engaged with the website.	Sum-up tracked via Google Analytics	Year 2 target: 400-700/month End of project target: 700-1000/month	799
KPI8.1d Content update on Cyberwiser.eu	Number of content pieces updated on www.cyberwiser.eu includes News, Events, information services and others type of content based on both trends in the cyber space landscape and the evolution of the media platform.	Sum up of content pieces tracked thanks to cyberwiser.eu CMS	Year 2 target: 120 End of project target: 240	144
KPI8.1e Newsletters	Number of newsletter sent to the WISER registered users	Sum-up tracked via cyberwiser.eu CMS	Year 2 target: 5 End of project target: 10	6

KPI8.1 F Press & Media materials	Number of printed & online materials that includes various formats used to widely promote WISER (PRs, Flyer, Poster etc.)	Sum-up tracked via cyberwiser.eu CMS	Year 2 target: 5 End of project target: 10	24
---	---	--------------------------------------	---	----

Table 1 - WP8 - KPI8.1: Web and social outcomes

Name	Definition	Measurement methods	Thresholds	Current Value
KPI8.2a Registered users	Number of users registered to www.cyberwiser.eu	Sum-up tracked via cyberwiser.eu CMS	Year 2 target: 750 End of project target: 1500	198
KPI8.1b Twitter followers	Number of Twitter followers	Sum-up tracked via Twitter Analytics	Year 2 target: 150 End of project target: 350	310
KPI8.2c Tweets sent	Total number of Tweets sent	Sum-up tracked via Twitter Analytics	Year 2 target: 240 End of project target: 480	1447
KPI8.2d LinkedIn Connections	Number of LinkedIn connections	Sum-up tracked via LinkedIn Analytics	Year 2 target: 250 End of project target: 500	992
KPI8.2e LinkedIn Post	Total number of LinkedIn Updates and Posts sent	Sum up of LinkedIn updates and posts	Year 2 target: 120 End of project target: 240	198
KPI8.2f Overall Community Database (include registered users, Twitter followers & LinkedIn connections)	Any person, that may or may not represent an organisation, that has been identified as a potential target audience member and can be targeted and contacted as such.	Sum up of the total contacts. The database is being constantly updated by Trust-IT	Year 2 target: 900 End of project target: 2350	1500
KPI8.2g EAPs active	Number of Early Assessment Pilot playing an active role into WISER project.	Sum up of EaPs tracked thanks to the website CMS	Year 2 target: 2 End of project target: 10	11

Table 2 - WP8 - KPI8.2: Target market outreach & stakeholder response

Name	Definition	Measurement methods	Thresholds	Current Value
KPI8.3a Data Collection	Number of content pieces published under section “Insights” of www.cyberwiser.eu	Sum up of content pieces tracked via cyberwiser.eu CMS	Year 2 target: 25 End of project target: 50	117

Table 3 - WP8 - KPI8.2: Target market outreach & stakeholder response

Name	Definition	Measurement methods	Thresholds	Current Value
KPI8.4a Leads generated	Potential WISER users showing concrete interest. We have included them here to measure the effectiveness of the communication activities in generating interest in WISER outputs.	Included in and tracked as part of the Overall Community Database The database is being constantly updated by Trust-IT	Year 2 target: 10 End of project target: 50	2
KPI8.4b Performed CyberWISER Light Sessions	Number of times the Cyber WISER Light service is used.	Sum-up tracked via cyberwiser.eu CMS	Year 2 target: 240 End of project target: 480	157
KPI8.4c Commercial agreements (Basic & OR Advanced Session)	Number of formal agreements to use the Essential or Plus services.	Sum-up tracked via WP8 activities	Year 2 target: 25 End of project target: 50	1

Table 4 - WP8 - KPI8.4: Market prospects, leads generated & commercial agreements

1.4 Overall KPIs status and mitigation actions

The overall status of KPIs in WP8 is quite good shape, with several KPIs that already have reached their target before the end of the project.

However, given the ambitious KPIs set, WISER is struggling in terms of numbers of people reached by its services, in particular in relation to the user registered to the website (KPI8.2a) and in the numbers of the Performed CyberWISER Light Sessions (KPI8.4b), which are good but still remain low compared to the initial expectations.

The WISER consortium is therefore working on a series of mitigation actions to improve these indicators with effort from all partners.

Among those actions:

- Promote WISER at a national level, by participating in different events across Europe linking the WISER services with guides, glossaries and other promotional material in national languages in order facilitate understanding of cyber risks and foster risk management but also awareness of the new regulations and how they affect all businesses.
- Promote WISER at a business level, leveraging on the business network that each partner has, making sure that the right message is delivered to the right people at the right time.
- Promote WISER to its peer community, leveraging on the synergies with other EU funded projects established in T6.5, to boost dissemination and outreach.

1.5 Community Database

A WISER community database made up of the five major stakeholder/target audience as defined in section 2.3 for communications, marketing and disseminating results is regularly updated and monitored to keep track of how the community is growing and categorise relevant stakeholders particularly the potential segments considered for the uptake of the WISER tools.

The number of verified and relevant contacts³, is incremented through:

- Partner efforts in recruiting new community members.
- Web platform registration and newsletter subscriptions.
- Social and professional networks.
- Event participation and organisation.
- Synergies and strategic collaborations.

For the project's database, a final target of over **2350** contacts at the end of the project has been defined. The overall community database will include registered users, Twitter followers and LinkedIn connections. The database is being constantly updated by Trust-IT and is being exploited by WISER to create awareness and consolidate a loyal user base for the WISER tools and services.

The contacts are profiled based on their expertise and type of organisation for tailored messaging and content delivery.

Based on the profiling the different categories of contacts classified as specific WISER target audiences and are engaged through the most effective communication channels, tools and formats.

³ Any person, that may or may not represent an organisation, that has been identified as a potential target audience member and can be targeted and contacted as such.

1.6 A Joint Effort

The communication plan is a joint and coordinated effort among all WISER partners. Every partner contributes to the actions foreseen in the communication plan, in proportion to the effort allocated to each of them in WP8. Specific details on every partner commitment on single actions and activities will be required during the regular WP8 conference calls.

The WISER communication strategy (T8.1 – Marketing & Communications; T8.2 – Stakeholder Engagement and Community Development) creates the mechanisms for stakeholder engagement from the very outset and making sure WISER stays up to speed with a fast-evolving landscape. It also supports and paves the way for the other tasks with WP8: T8.3 - Market and Exploitation; T8.4 – Business Models; T8.5 – Socio-economic impact tool development, by providing a community of prospective users of WISER services, defining its value proposition and sharing market data and best practices.

More broadly, the communications strategy is designed to support all technical WPs (2-5) in disseminating results achieved especially to peer R&I actions and other technical communities.

Specifically, it ensures close interaction with WP6 “Pilots” in relation to Task 6.5: Synergies and international liaison on best practices, particularly the analysis of national cyber security strategies and policy priorities related to national information and security (NIS) systems in the drive towards a secure digital single market. Other key synergies are focused on relevant initiatives around the globe, especially the work of the US National Institute of Standards and Technology (NIST), whose cyber security framework represents a global reference document.

Close interaction with WP7 “Market Validation and Roll-Out to Other Verticals” is a central part of the communications strategy relating to community building and stakeholder engagement, with the aim of ensuring wide uptake of WISER tools and services across a diverse set of verticals, taking into account market conditions and potential and user validation.

Partner commitment to the Communication Plan therefore extends to each and every one of these strategic activities.

1.7 A Living Document

Communication is by definition dynamic. To be effective, it has to take into account ever-changing trends and market conditions, ever more so in the cyber space. The WISER Communication Plans are therefore conceived as “living documents”, taking into account the fast-paced landscape and emerging market opportunities. Trust-IT makes the commitment to amend and update the plan as such opportunities present themselves, sharing updates with the WISER partners whenever and wherever they affect the communications strategy through regular virtual meetings and communications.

2 WISER Package Offers and Markets

2.1 WISER Cyber Risk Monitoring Services

The extended suite of tools and services (see Figure 2) that WISER delivers to its market targets of small businesses, large companies and public sector organisations are based on three different modes of operations, branded as:



Figure 2 - Branding of CyberWISER product packages

The branding of the suite of WISER outputs complements its distinctive look and feel across the broad set of communication tools used by WISER, with the core concept of the key as a symbol of security

while highlighting the various levels of the services using progress bar icons. The services are also highlighted through different colour schemes making it easier for the user to distinguish and recognise the various service options.

CyberWISER Light

CyberWISER Light, the first service rollout of WISER was made available in March 2016 to the early assessment pilots and selected organisations within the WISER network. CWL is accessible from the WISER media platform: www.cyberwiser.eu.

Main benefit: increase the awareness of cyber-risks for their businesses through self-assessment. It is a user-friendly approach for small businesses and organisations of all sizes that lack the time, money and skills to invest in cyber risk management. SMEs and organisations of all sizes can get a first, high-level view of their cyber risk exposure free of charge and with minimum investment in time and human resources.

There are two parts to the service:

1. A questionnaire that gives SMEs and organisations a first, high-level view of their cyber risk exposure based on 28 questions collecting and assessing basic information about the organisation and its cyber risk exposure
2. A vulnerability test which detects the vulnerabilities present in a specific web/infrastructure and offers a high-level rough estimation of cyber risk exposure basing on the importance for the company business of the data potentially affected in such target by the vulnerabilities found.

CYBERWISER Essential

While in the CyberWISER Light the issues detected have rather to do with the vulnerabilities of the infrastructure and likely problems that might arise in the short term, in the basic mode of operation this is extended to the detection of issues already happening and informing the user.

This solution offers simple functionalities and a basic repository of standard risks, vulnerabilities and threat models and simple cyber risk patterns that can be instantiated by following a lightweight approach to analysis.

CyberWISER Essential offers the assessment of the risk based on not only the business and ICT variables indicated by the user in an upgraded version of the one used in the CyberWISER Light, but also on the information obtained from the cyber climate of the user's infrastructure/web server which is analysed and monitored thanks to sensors installed at the network layer level.

The assessment of the impact of cyber risks is based on a set of economic factors with minimal coverage. Decision support is supported by the provision of a list of mitigation measures responding to the risks detected.

Main benefit: SMEs and ICT systems in general are able to detect, monitor and manage the vulnerabilities and issues already happening in their systems and draw a plan about mitigation actions thanks to the Decision Support System

CYBERWISER Plus

The most advanced solution offers a real-time platform serving as a Risk Platform as a Service (RPaaS) to operate in real time providing online feedback about risk exposure mitigation and transfer, smart alerts/push notifications and countermeasures/mitigation actions.

CyberWISER Plus allows users to select a range of sensors or integrate their own according to their particular needs, sending the events to the remote WISER monitoring platform by means of the agreed communication protocol, leaving the costly correlation and analysis tasks to it.

Main benefit: critical infrastructure or highly complex cyber systems can benefit from on-demand services for real time and cross-system assessment of vulnerabilities and threats.

CyberWISER Plus not only suggests mitigation strategies but also offers the possibility of carrying out a cost-benefit analysis of the identified strategies and comparing them in order to choose the best one.

Figure 3 below presents the various levels of sophistication associated with each WISER service.

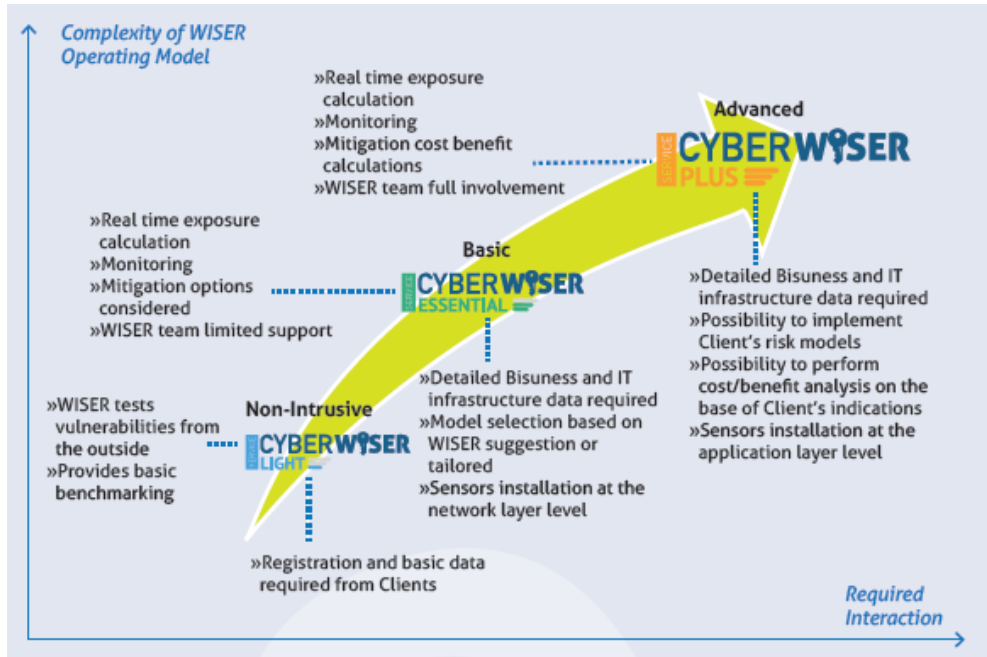


Figure 3 - The WISER 3-level offer (CyberWISER Light, Essential, Plus)

2.2 WISER Cyber Risk Awareness Free Services

WISER is also offering free services (see Figure 4) to facilitating the uptake of a cybersecurity culture to enhance business opportunities and competitiveness among Europe. This is done by allowing free access to the CyberWISER Cartography and to the Socio Economic Impact Tool:



Figure 4 - WISER Cartography & Socio Economic Impact Tool

CyberWISER Cartography

The WISER cartography takes a specific approach to member state progress on the adoption of the NIS Directive, by first describing the current and updated state of the art of every EU national cybersecurity strategy (such as objectives, legal conditions, operational capacities etc.) and analyzing their current implementation of the NIS directive (CERTs/CSIRTs presence, best practices, monitoring systems etc.). To complement this work, individual interviews with CSIRTs/CERTs representative has been carried out with the aim to fill knowledge gaps and helping to identify best practices within different cultural environments across the EU.

Main benefit: The interactive map provides a bird's eye view of the European landscape and offers

insightful accurate and practical information for businesses and organizations who wants to have a clear understanding of their national cyber security progress in terms of regulatory gaps, international co-operation and best practice adoptions.

CyberWISER Socio Economic Impact Tool

This user-friendly online tool helps users to estimate the economic and non-economic impact of cyber attacks. Users, whether SMEs or small IT teams, simply need to complete the online questionnaire, which addresses intangible, but very important, topics related to cyber risk.

Main benefit: It is essential that small businesses develop the capability to assess their cyber risk exposure and consequences from a socio-economic viewpoint. This is especially important for micro business owners that do not normally have IT specialists or cyber security staff. Being part of the WISER “light” approach, the tool is designed to be user-friendly and available as a free online tool. This tool also demonstrates the benefits of using more advanced and complete WISER service, i.e. CyberWISER Plus, in cases where risk exposure and impact are both high to very high, by providing a more complex and complete estimation of the socio-economic impact of cyber risks.

2.3 WISER Markets and Target Audiences

WISER targets its messaging to five main target audiences:

- **Target 1:** micro (less than 10 employees), small- and medium-sized businesses (up to 250 employees) with an increasing number of them expected to become digital businesses⁴.
- **Target 2:** large companies (over 250 employees).
- **Target 3:** the public sector, e.g. IT decision makers, Chief Information Security Officers especially small IT teams within these organisations.
- **Target 4:** policy stakeholders (policy makers, R&I actions, international standards bodies).
- **Target 5:** the general public.

The micro firm sector, which is growing rapidly and generating significant economic impact⁵ represents a major market target for WISER. We therefore adopt a “Think Small First” approach as more and more firms are expected to become digital over the next few years. This is also in line with Europe’s strategy for a single digital market.

The table below shows the KPIs for the overall community building, indicating the specific targets for each group, with a priority given to the private sector as key customer segments (e.g. small firms (SMEs) and large companies).

WISER’s Target Audiences and dedicated effort

Tailored activities for each target audience are delivered based on the dedicated effort breakdown in table 5 below, where Micro, Small and Medium-Sized Organisations (Small Firms) are identified as a key focus.

ID	Target Audience	Dedicated effort (%)
TA1	Micro, Small and Medium-Sized Organisations (Small Firms)	40%
TA2	Large Companies	25%
TA3	Public Sector	15%

⁴ As most SMEs in Europe and most new firms are micro businesses, we refer to this category as “Small Firms”. It is also the group that lacks IT security experts, time and money to dedicate to cyber security strategies. WISER has the potential to impact positively on this group.

⁵ For example, 76% of all UK businesses are micro firms, contributing 10% to the GDP. It is estimated that getting all micros online could generate €25bn to the UK economy. See <http://www.pictfor.org.uk/how-to-get-the-smallest-businesses-online/>.

TA4	Policy and Standards Bodies	10%
TA5	General Public	10%

Table 5 - KPIs for Target Audiences

3 Year Two Achievements: Multi-channel and Multi-stakeholder Engagement

Strategy for year 2: Ensure that WISER engagement with its various stakeholders takes place on multiple levels and across different channels and formats. The overall aim is to start building a marketplace for the WISER tools and services on the one hand, and connect the WISER community to a growing body of knowledge tailored to the needs of busy professionals. Key to this is creating trust in WISER and building up a loyal following.

To this end, WISER defines, promotes and communicates strategic business cases and concrete benefits for real-world issues based on a twofold strategy, that is, continuous online engagement and regular face-to-face engagement at selected events.

Face-to-face interaction serves several purposes: ensuring WISER visibility, communicating benefits for target audiences, gaining insights into market needs, and making new contacts as part of the community development. Event participation also includes sharing technical advances with peer developer communities. All WISER partners are requested to report back on new contacts, visibility and concrete follow-up actions, e.g. new leads and target group expectations.

Regarding online engagement, activities on social and professional channels link the WISER community to the informative and educational content on the media platform, engaging in debate on common interest and offering live updates and trends on the cyber security landscape.

In the first 24 months of the project, engagement formats have included practical and policy guides, video clips, advertising banners, brochures, collaterals, and factsheets on cyber security that capture trends, raise awareness on the business benefits of a strong cyber security posture, guiding organisations of all sizes in implementing more effective risk management by adopting WISER services and tools.

Below, we report the main results for the media platform, social networks, press and media campaigns, direct engagement through events, and webinar planning.

3.1 Media Platform and Content Creation

Strategy: The WISER media platform, operated at www.cyberwiser.eu plays a key role in communicating the WISER value proposition to key customer segments and stakeholders.

Since the start of WISER, the project has carried continuous communications, setting up the media platform (www.cyberwiser.eu) and social networks, creating collaterals and creating media campaigns on the project launch. As part of the project user-centric approach, the [cyberwiser.eu](http://www.cyberwiser.eu) web platform is currently undergoing a restructuring aimed at increasing the visibility on the WISER Services. The evolution of the platform will be increasingly towards showcasing the suite of WISER tools and services as part of the strong go-to-market project strategy.

Strategy for informative and educational content: Given the increasing importance of EU regulatory changes, WISER has decided to implement a new section called “Policy Guides” on the media platform and social media channels, with the aim of assisting organisations in understanding compliance with new EU regulation around Network Information and Security Directive (NISD) and Data Protection Regulation Reform (DPRR), whereby state-of-the-art cyber risk accountability becomes businesses’ top priority.

A specific Essential Guide on the NIS Directive (see Figure 5) and its implications for organizations and general public has been created make available on a dedicated section of the project website

(<https://cyberwiser.eu/insights/policy-guide>) and translated also in [French](#), [Italian](#), [Spanish](#) and [Slovenian](#).

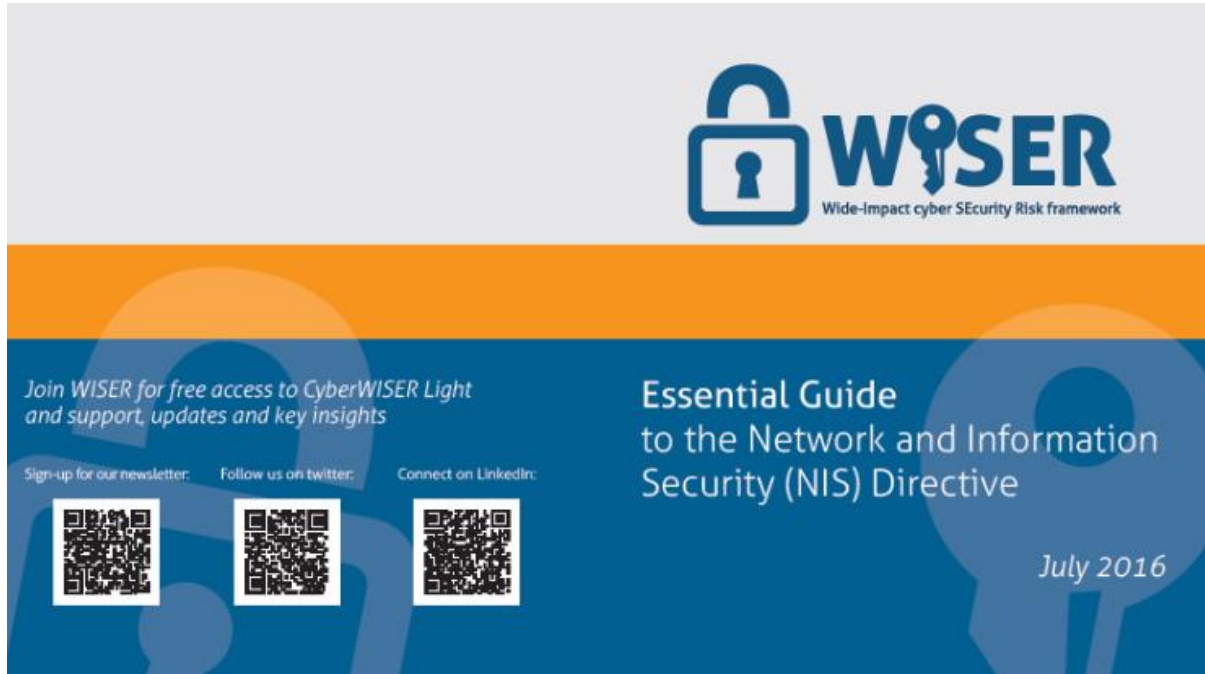


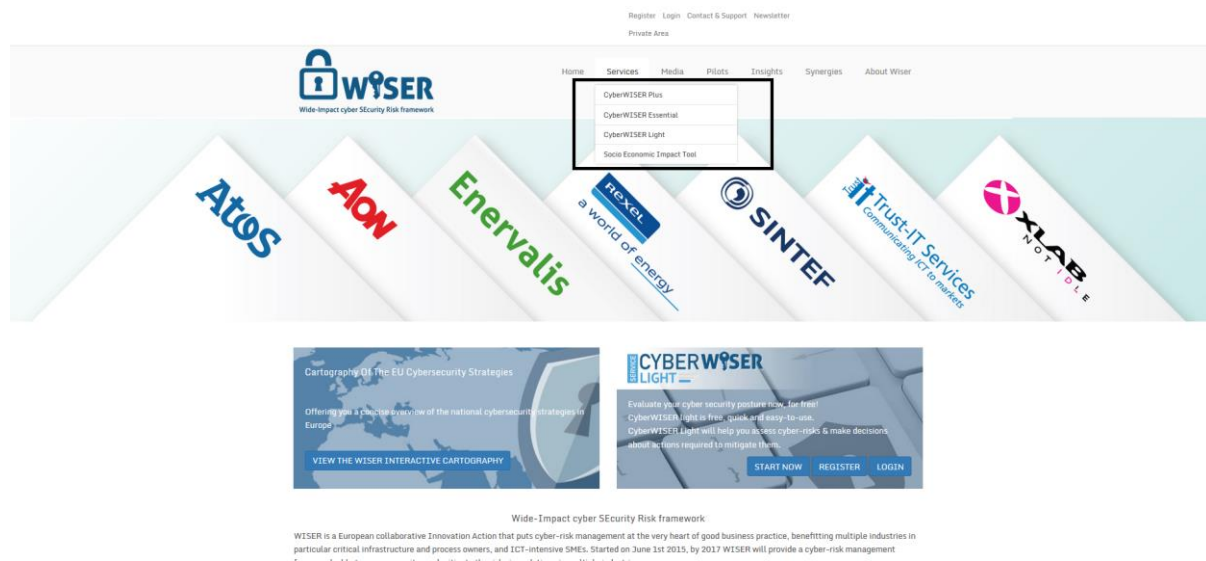
Figure 5 - Essential Guide to the NIS Directive

This new section links to the Market Watch of industry best practices relating to the implementation of policy priorities and regulations, e.g. Computing Response Teams (C-CERTS). This new educational WISER service draws on Task 6.5 and findings from D6.2 - Best Practices and Early Assessment Pilots, Final Version (May 2016).

The purpose of the practical guides on new EU regulations is to assist organisations affected to make timely adjustments to their cyber security strategies based on new compliance regulations.

As such, this new web service will complement current services such as the **Market Watch**, which tracks best practices within the public and private sector in terms of responding to the fast-evolving cyber threat landscape.

Achievements: The WISER web platform is now hosting the access to the full suite of the WISER services (CyberWISER Light, CyberWISER Essential, CyberWISER Plus, Socio Economic Impact Tool, Cartography) as planned in the first two versions of the Wiser Communication Plan. Figure 6 below shows the complete list of services hosted on the WISER web platform.


Figure 6 - www.cyberwiser.eu

The website www.cyberwiser.eu has been updated with more than 73 news content highlighting different topics issues, news and strategies emerging from the fast changing landscape of cyber security. WISER ensures that content creation is tailored to its different target audiences. Table 6 below shows a sample of content created and uploaded in the first 24 months.

Stakeholder(s): SMEs/Large companies	
EU firms slow in detecting cyber attacks: How WISER can help	https://cyberwiser.eu/news/eu-firms-slow-detecting-cyber-attacks-how-wiser-can-help
Cybersecurity at the top of the agenda for financial services	https://cyberwiser.eu/news/cybersecurity-top-agenda-financial-services
Helping SMEs in their cyber security journey	https://cyberwiser.eu/news/helping-smes-their-cyber-security-journey
Helping SMEs to boost their cyber security with CyberWISER Light	https://cyberwiser.eu/news/helping-smes-boost-their-cyber-security-cyberwiser-light
Stakeholder(s): Public Sector	
New EU Guidelines on Data Protection Impact Assessment	https://cyberwiser.eu/news/new-eu-guidelines-data-protection-impact-assessment
Commission's top scientific advisers publish opinion on cybersecurity in the Digital Single Market	https://cyberwiser.eu/news/commissions-top-scientific-advisers-publish-opinion-cybersecurity-digital-single-market
Stakeholder(s): Policy and Standard Bodies	
Commission's top scientific	https://cyberwiser.eu/news/commissions-top-scientific-advisers-

advisers publish opinion on cybersecurity in the Digital Single Market	publish-opinion-cybersecurity-digital-single-market
EU Commission releases report on Cyber Security in the Energy Sector	https://cyberwiser.eu/news/eu-commssion-releases-report-cyber-security-energy-sector
UK releases Civil Nuclear Cyber Security Strategy	https://cyberwiser.eu/news/uk-releases-civil-nuclear-cyber-security-strategy
NIST Releases Update to Cybersecurity Framework	https://cyberwiser.eu/news/nist-releases-update-cybersecurity-framework
Key changes with GDPR	https://cyberwiser.eu/news/key-changes-gdpr
Stakeholder(s): General Public	
2017 cyber crime trends.	https://cyberwiser.eu/news/ncsas-five-digital-dos-2017
Key GDPR Issues InfoSec Professionals should address MARKET WATCH – industry best practice/policy implementation	https://cyberwiser.eu/news/key-gdpr-issues-infosec-professionals-should-address
IoT cyber risk factors 2017	https://cyberwiser.eu/news/iot-cyber-risk-factors-2017
WISER Achievements	
WISER presented at Gestion Radio	https://cyberwiser.eu/news/wiser-presented-gestiona-radio
Launch of CyberWISER framework: Monitoring your cyber risks in real time	https://cyberwiser.eu/news/launch-cyberwiser-framework-monitoring-your-cyber-risks-real-time

Table 6 - Sample of Content Creation in Year Two

3.2 Social Media Networks

Strategy for year 2: Dedicate effort to online engagement with integration of social media networks like Twitter⁶, and LinkedIn⁷ on the media platform, allowing users to share web content directly from the website. Convey important messages to the diverse set of target audiences, including real-time updates from events and webinars. Ensure social networks form a central part in the CyberWISER Essential & Plus launch campaign also in terms of recruiting users potentially interested in the WISER offer, tailoring messages to different audiences.

Specifically:

- Twitter is used to provide brief real time updates, news flashes and live event reporting, while also engaging in online debate. A regularly updated pool of relevant hashtags and handles is used to help draw attention to key WISER-related themes and recruit new followers.
- LinkedIn offers WISER access to professionals across current and new sectors, helping to build up its community, while conveying key messages on the benefits of WISER, landscape trends and important policy updates.

Achievements: WISER has selected one key social network, Twitter and one professional channel, LinkedIn, to consolidate its online presence, communicate its outputs and results and build its

⁶ <https://twitter.com/cyberwiser>.

⁷ <https://www.linkedin.com/grps/CyberWISER-8411544/about>.

community. Table 7 below summarise the KPIs achieved in relation to the first version of the Communication Plan:

Name	Definition	Measurement methods	Thresholds	Current Value
KPI8.1b Twitter followers	Number of Twitter followers	Sum-up tracked via Twitter Analytics	Year 2 target: 150 End of project target: 350	310
KPI8.2c Tweets sent	Total number of Tweets sent	Sum-up tracked via Twitter Analytics	Year 2 target: 240 End of project target: 480	1447
KPI8.2d LinkedIn Connections	Number of LinkedIn connections	Sum-up tracked via LinkedIn Analytics	Year 2 target: 250 End of project target: 500	992
KPI8.2e LinkedIn Post	Total number of LinkedIn Updates and Posts sent	Sum up of LinkedIn updates and posts	Year 2 target: 120 End of project target: 240	198

Table 7 - WP8 - KPI8.2: Target market outreach & stakeholder response

WISER's continuous activity on Twitter & LinkedIn has increased the numbers of tweets, connections and followers but also the overall impressions of the WISER messages. With contributions from partners, several promotional, informative and direct messages have been sent also in national language (see Figure 7).



Figure 7 - Example of messages in national language

A specific crash action on LinkedIn has involved the direct engagement of CEOs, CISOs, CTOs, Security Manager and IT professionals to recruit potential users interested in the WISER services and has brought the WISER LinkedIn profile to more than 990 connections (see Figure 8).

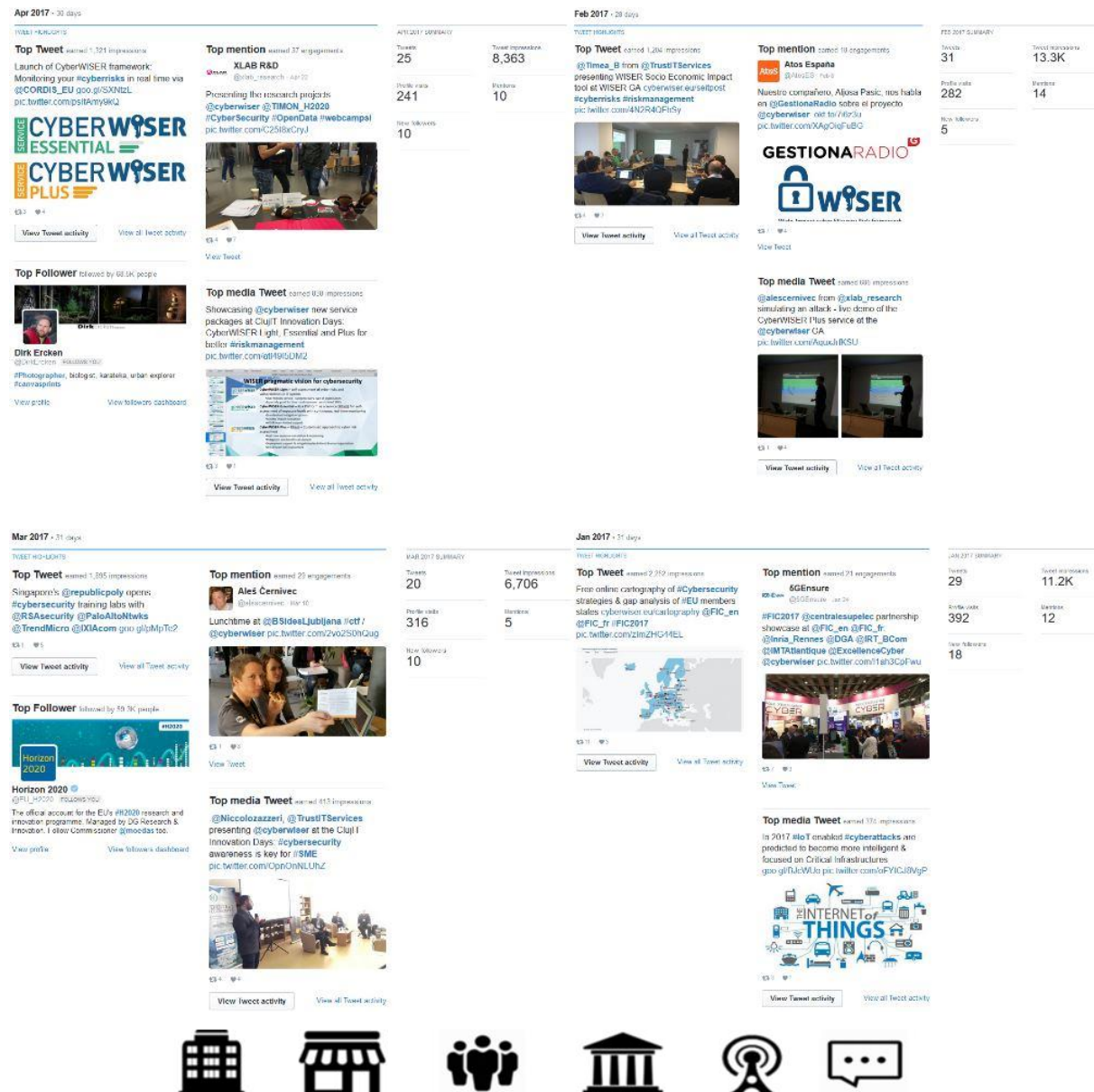


Figure 8 - Visibility and Impact on Social Media

Messaging focuses on specific targeted insights on security and risk management, to raise awareness on the key role of cyber security in Europe and worldwide as well as promoting best practice and practical tools to help targeted audiences meeting their specific needs on IT security sector (see Table 8).

Target Audiences	Tweet posted	Engagement
1 – SMEs, 5 - General Public	Make cyber #riskassessment a top priority for your #business today with CyberWiser Light https://www.youtube.com/watch?v=yUL4G6k6J9s ...	Impressions: 2404 Total Engagements: 31
4 - Policy Stakeholders, 5 - General Public	Rossella Mattioli #ENISA explains the mission & actions of @enisa_eu for #cybersecurity , @Cyberchallenge , #CyberEurope @JuliaSoftware pic.twitter.com/DOUsZnibTs	Impressions: 3847 Total Engagements: 20
2 - Large Companies	Survey of the oil & gas industry by @TripwireInc reveals only 31% of org. felt capable of detecting #cyberattacks ow.ly/XWEwz	Impressions: 1961 Total Engagements: 23
3 – Public sector	Free online cartography of #Cybersecurity strategies & gap analysis of #EU members states https://www.cyberwiser.eu/cartography @FIC_en @FIC_fr #FIC2017 pic.twitter.com/zlmZHG44EL	Impressions: 4049 Total Engagements: 67

Table 8 - Targeted Tweet Examples

LinkedIn Content

A sample of messaging on LinkedIn includes:

- The British Chambers of Commerce digital survey shows that 1/5 businesses have fallen victim to a cyberattack in the past year. (104 views) (March 2017).
- Guidelines for SMEs on the security of personal data processing (93 views) (January 2017).
- Launch of CyberWISER framework: Monitoring your cyber risks in real time (59 views) (April 2017).
- NCSA's Five Digital To Dos for 2017 (90 views) (December 2016).

3.3 Events

Events are identified for their timeliness with WISER outputs, topic and audience relevance. Participation spans presentations, panel debates, promotional stands, poster displays, remote participation and the distribution of project promotional material (roll-up banners, brochures, etc.) for focused and effective communication, dissemination and engagement outcomes, with live reporting via twitter, updates and blogs on LinkedIn.

Achievements: Table 9 below provides a summary of WISER visibility and related web and social media activities at different market targets and stakeholder events.

Target Audience Categories	Event Name and Location	WISER Actions and Visibility
4 Policy stakeholders - 5 General Public	CIRAS project final conference 08 June 2016, Katowice, Poland	Antonio Alvarez Romero, ATOS presented an overview of the WISER project and presented CyberWISER Light service as a first, concrete outcome.
3 – Public Sector – 4 Policy stakeholders	Trust in the Digital World (TDW) conference 15-16 June 2016, Netherlands	Fernando Carmona promoted the WISER project through discussions and the distribution of our latest flier.
1 – Small Firms; 2 – Large Companies – 3 – Public Sector	DSS ITSEC 2016 27 October, 2016, Riga, Latvia	WISER and its tools were presented at DSS ITSEC 2016 in Riga by Antonio Alvarez Romero (ATOS)
1 – Small Firms; 2 – Large Companies	4th International Workshop on Risk Assessment and Risk-driven Quality Assurance 18 October 2016, Graz, Austria	Gencer Erdogan (SINTEF) presented WISER and received valuable inputs in the economic and social impact assessments as useful per se but also as a tool used in companies as an integral part of the cyber risk assessment, helping prioritise mitigation actions
1 – Small Firms; 2 – Large Companies - 4 Policy stakeholders - 5 General Public	Cluj Innovation Days 2017 30-31 March 2017, Cluj Napoca, Romania	Niccolò Zazzeri (Trust-IT) presented the full suite of WISER services
1 – SMEs, 5 - General Public	WebCamp 2017, 22 nd April, Ljubljana	Marta Štimec, Aleš Černivec (XLAB) promoted the WISER project through discussions and distribution of fliers.
4- Policy stakeholders 3 - Public sector	Cloud Security Alliance SEE Summit 2017 and BSides, security driven information security conference, 9 and 10 March 2017, Ljubljana, Slovenia	Anže Žitnik (XLAB) promoted the WISER project through discussions and distribution of fliers.

Table 9 – WISER Event Presence

3.4 Media Visibility and Publications

3.4.1 CyberWISER Essential & Plus Launch Campaign

Press and media campaigns occur at specific moments of the project, including project launch and major milestones in delivering new, market-ready services. Campaign planning is an all-partner activity with specific tasks assigned based on effort allocated, leveraging partner expertise in producing compelling messages and regularly updated press and media database. Such channels also include radio and TV interviews, and conference Press Release services.

Strategy: Define and implement a large-scale campaign for the official launch of the WISER advanced services (CyberWISER Essential & Plus) to relevant media, business associations and businesses following a soft launch to WISER pilots and selected organisations. Use the large-scale campaign as the basis for future press and marketing campaigns. The communication campaign has mainly targeted on Editor, Journalists, Media channels, ICT/Security magazine, SMEs, associations and potentially interested users.

Table 10 below summarizes the number of users contacted during the first phase of the campaign:

Type of Contact	Country	Nr. of contacts
<i>Editor/Journalist</i>	UK, Netherlands, Belgium	500
<i>SMEs/Association</i>	UK, Netherlands, Italy, Germany, Spain, France, Portugal, Belgium, Ireland, Poland	85
<i>Cybersecurity/Risk management Twitter/LinkedIn Users</i>	UK, Netherlands, Italy, Germany, Spain, France, Portugal, Belgium, Ireland, Poland	380

Table 10 - Contacts for the CyberWISER Essential & Plus campaign

The campaign has involved:

- [Master PR](#) (English version) announcing the launch of CyberWISER Essential & Plus.
- Translation of the [PR into Italian](#).
- Translation of the [PR into Slovenian](#).
- Translation of the [PR into Spanish](#).
- Translation of the [PR into French](#).
- Translation of the [PR into Dutch](#).
- Translation of the [PR into Norwegian](#)
- Distribution to media IT and sector-specific media channels.
- Distribution to SMEs NTAs and business associations.
- Distribution to WISER business community.

Social Media

- LinkedIn Blog and weekly reminders.
- Twitter posts targeting also SME and business associations.
- Direct messages via Twitter in English, Spanish Italian & Slovenian

Clippings currently sourced – CyberWISER Essential & Plus

- http://cordis.europa.eu/news/rcn/139715_it.html
- www.slovenianbusinessclub.si/podjetje-xlab-kot-integrator-varnostnih-mehanizmov/
- <http://www.insurancetrade.it/insurance/contenuti/tecnologie/6804/monitorare-il-cyber-risk-in-tempo-reale>
- <http://www.intermediachannel.it/progetto-wiser-due-nuove-soluzioni-per-monitorare-e-gestire-i-rischi-informatici-in-tempo-reale/>
- <http://www.asefibrokers.com/notizie/dal-progetto-wiser-due-soluzioni-la-gestione-tempo-reale-dei-rischi-informatici>
- <https://ilbroker.wordpress.com/2017/04/12/cyberwiser-essential-e-cyberwiser-plus-due-soluzioni-innovative-per-monitorare-e-gestire-i-rischi-informatici-in-tempo-reale/>
- <https://www.assinews.it/04/2017/cyberwiser-essential-cyberwiser-plus-due-soluzioni-innovative-monitorare-gestire-rischi-informatici-tempo-reale/660038900/>
- <http://www.dataversity.net/launch-cyberwiser-framework-monitoring-cyber-risks-real-time/>
- <http://www.ciodive.com/press-release/20170414-launch-of-cyberwiser-framework-monitoring-your-cyber-risks-in-real-time/>
- <http://www.tuttointermediari.it/?p=27584>
- <https://hakin9.org/launch-cyberwiser-framework-monitoring-cyber-risks-real-time/>
- http://cordis.europa.eu/result/rcn/188757_en.html

Clippings currently sourced – CyberWISER Light

- http://cordis.europa.eu/news/rcn/133094_it.html
- <https://www.globalsecuritymag.fr/Cyber-Wiser-Light-Service-Une,20160531,62528.html>
- <http://www.bitmat.it/blog/news/56489/cyberwiser-light-la-soluzione-online-di-cybersecurity-per-le-pmi>
- <http://www.cyberdefensemagazine.com/cyberwiser-light-helping-european-firms-get-smart-about-cyber-security/>
- <http://cso.computerworld.es/tendencias/ciberseguridad-inteligente-al-alcance-de-todas-las-empresas-cyberwiser-light>
- <https://pentestmag.com/cyberwiser-light-helping-european-firms-get-smart-cyber-security/>

The full list of clippings actually published from the CyberWISER Light campaign as well as from the CyberWISER Essential & Plus campaign can be found at this link: <https://cyberwiser.eu/coverage>

3.4.2 Articles and Publications

In the first 24 months of the project, WISER has produced several articles.

- Cloudscape Brazil 2016 Position Paper: *How WISER is paving the ground for cyber security challenges in the Digital Single Market*, Author: ATOS; editor: Trust-IT, March 2016⁸.

⁸ <http://cloudscapeseries.eu/content/how-wiser-paving-ground-cyber-security-challenges-dsm>.

- Article for ERCIM News Special Issue on cyber security (July 2016): Automating website vulnerability detection in CyberWiser Light Technology. Co-authors: Anže Žitnik, Antonio Álvarez Romero, Stephanie Parker.
- *Launch of CyberWISER framework: Monitoring your cyber risks in real time*⁹, Contributed by XLAB
- *WISER Result In Brief*¹⁰, Contributed by Trust-IT

4 Communication Plan for last six months of WISER

4.1 Strategic goals for 6-month WISER sprint

The overriding strategic goal of WP8 is to boost uptake of CyberWISER service packages by SMEs and also to support the portability to verticals other than the current pilots (financial services – insurance and energy – supply and smart grids), thus also supporting WP7. Therefore the 6-month plan revolves around three pillars:

- a complete product range for major marketing campaigns
- portability to other verticals for verification: Manufacturing, Transportation, ICT, Healthcare and connected devices, Public Administrations, in addition to a wide pool of SMEs that also but not only operate in these verticals
- a business model to be tested

The WP8 communication strategy focuses on intensified activities including:

- Messages to main targets
- Engagement with multipliers (e.g. Business associations and Cyber security Clusters)
- Media Kits including channels targeting the stakeholders in each vertical identified
- Direct engagement with targets through event participation
- S.M.A.R.T. social media campaigns
- Updated and new sections on www.cyberwiser.eu
- Teaser for the new CW-SEIT targeting SMEs and verticals followed by the launch of this tool and dedicated web section, also with the aim of helping SMEs prepare for the GDPR
- Promotional material that also includes opportunities for verticals to come on board as users and updated postcards on CyberWISER service packages inserted into a small folder that can be packaged for different stakeholders in a “mix-and-match” fashion.

4.2 Support of Portability to Verticals

As per DoA, WISER has carried out a detailed portability analysis in WP7, leading to the identification of 5 main verticals for the roll-out of the complete WISER offer:

Transportation, Healthcare and medical devices, ICT, Manufacturing, Public administrations.

A campaign draft for each verticals has been produced with all partners' commitment.

Partner networks and media relations play a key role in reaching these verticals, so participation at targeted events will be key to collect new users and testimonials as part of the go-to-market strategy.

Among the initial set of actions defined, dedicated web pages will be produced for each verticals, putting greater emphasis on the importance of cyber risk management as the first fundamental step towards a better IT security posture as well as clearly stating the benefits that the WISER services can bring to each verticals.

⁹ http://cordis.europa.eu/news/rcn/139715_it.html

¹⁰ http://cordis.europa.eu/result/rcn/188757_en.html

4.3 Formats and Channels

Table 11 below summarizes the different sets of formats for engaging with different target audiences.

Formats	Description	Delivery Channels/Business Multipliers	Market targets & Audience categories ¹¹				
			1 ¹²	2 ¹³	3 ¹⁴	4 ¹⁵	5 ¹⁶
WISER flier	Fliers including the promotion of the services and tools as well as the project goals and achievements of the initiative. Distribution at relevant events.	Website, Events, Press & Media, Social media	√	√	√	√	√
Roll Up Banner/Posters	Pop up banner conveying core WISER messaging for visibility at events.	Events	√	√	√	√	√
Press Releases	Press releases produced at specific moments of the project distributed to Press & Media Channels	Website, Events, Press & Media, Social media	√	√	√	√	√
Interviews & Audio-visuals	Interviews with representatives of the WISER pilots as well as other key stakeholders.	Website, Press & Media, Social media	√	√	√	√	√
Newsletters	Delivery of newsletters with targeted content for the different stakeholders.	Website, Press & Media, Social media	√	√	√	√	√
Info graphics	As a visually appealing instrument to raise awareness on the different topics addressed as well as illustrate the benefits of WISER tools.	Website, Press & Media, Social media	√				√
Partner Promotional Kit	Partner-specific material is produced upon request to promote the initiative within their organisations and to their networks and channels, also in line with their organisational mission.	Website, Events, Press & Media, Social media	√	√	√	√	√

¹¹ It is intended that each market target will receive a tailored version of the various messaging formats

¹² Small firms.

¹³ Big Corporations.

¹⁴ Public Sector and IT Decision-Makers.

¹⁵ Policy and Standards Bodies.

¹⁶ European Citizens.

Formats	Description	Delivery Channels/Business Multipliers	Market targets & Audience categories ¹¹				
			1 ¹²	2 ¹³	3 ¹⁴	4 ¹⁵	5 ¹⁶
Give-aways	Appropriate give-aways such as bookmarks, cards, gadgets are produced during the life of the project to incentivise stakeholder engagement.	Events	√				√
Templates	Set of shareable presentations on WISER offer to facilitate effective and consistent messages.	Website, Events, Press & Media, Social media	√	√	√	√	√
Webinars	Interactive training and information sharing format that can accommodate a geographically diverse audiences at relatively low costs.	Website, Social media, Press & Media	√	√	√	√	√

Table 11 - Formats for Year Two

Webinars represent a new format for the remainder of the project, providing an opportunity to consolidate the WISER user base and to raise awareness amongst multiple stakeholders of WISER and its offer. The webinars will also serve the WISER overarching goal of increasing awareness in Europe and ensuring for all players a sophisticated, yet practical approach to cyber security via Risk Management, in quasi-real-time.

The first webinar was held shortly the launch of the CyberWISER Light service (May 2016) and also showcased the future opportunities for the WISER user community.

WISER will provide a set of webinars focused on the WISER service offer and aimed at supporting the service usage and uptake. The WISER webinars are a flexible as well as scalable training tool as these can accommodate a geographically diverse audience at relatively low costs.

4.4 WISER Event Planner

4.4.1 WISER Final Event

WISER will prepare a specific final event to widely promote its results at M29 (October 2017).

As per DoA, the event will be targeting policy decision makers, national governments and national cybercrime units, and industry experts will share outcomes and present the tools for re-use by the public and private sector.

At the time of completing this deliverable, two options are still kept open:

- **Plan A** – WISER presence at AON Lounge in FERMA Risk Management Forum 2017.
- **Plan B** – A series of WISER cyber security Workshops in EU members states.

Plan A – WISER presence at AON Lounge in FERMA Risk Management Forum 2017.

WISER would like to discuss excellence in research results in the Aon Lounge with dynamic demos and focused pitches with potential customers to help them find the right service packages for their company, with practical solutions in the complex cyberspace. WISER also plans to invite

cybersecurity experts as part of the agenda, offering an opportunity to inform participants on European policy priorities and national strategies.

WISER presents relevant findings and innovative solutions for cybersecurity, thanks to its approach that fuses risk management best practice with trust & security research. CROs, risk managers, and decision makers in the field are the ideal audience interested in taking a closer look to the “cybersecurity science” that provides practical solutions for businesses.

WISER is therefore highly complementary to the FERMA Forum 2017 new strategic vision and mission statement for a **“a world where risk management is embedded in the business model and culture of organisations”**.

Figure 9 shows the suggested agenda for the “WISER presence”

cybersecurity sprint #1	
11:00 – 11:10	Innovative paths to achieve cybersecurity for all – demo session on maxi screen, sprint #1 by Trust-IT Services
11:10 – 11:20	Demo presentation Q&A
11:20 – 11:45	Private pitch #1 – side meeting in 10-seat meeting room
cybersecurity sprint #2	
13:00 – 13:10	Cybersecurity models and tools – demo session on maxi screen, sprint #2 by ATOS
13:10 – 13:20	Demo presentation Q&A
13:20 – 13:45	Private pitch #2 – side meeting in 10-seat meeting room
cybersecurity sprint #3	
15:00 – 15:10	Real-time cyber risk management – demo session on maxi screen, sprint #3 by SINTEF
15:10 – 15:20	Demo presentation Q&A
15:20 – 15:45	Private pitch #3 – side meeting in 10-seat meeting room
Panel session and networking cocktail	
17:00 – 17:20	Panel – The future of cybersecurity innovation & the European Cyber Security Contractual Public-Private Partnership (cPPP). Moderated by Trust-IT, with representatives from: AON, Digital SME Alliance, ECSO, University of Oxford
17:20 – 18:00	Networking Cocktail offered by WISER

Figure 9 - WISER Final Event first draft agenda

PLAN B – A series of cyber security Workshops in EU members states. The Plan B involves a mini-series of workshops in different EU Member States. Each workshop will be facilitated by a local SME alliance, to ensure a significant participation and an appropriate focus on end-users, and the event will likely include also other Digital Security projects (e.g. CANVAS), to increase interest through concertation with other EC-funded initiatives.

Trust-IT has already successfully experimented this format in other context (ClujIT Innovation Days 2017) and preliminary agreements have been established with Cluj IT Cluster (Romanian ICT cluster) and AEI CITIC (Spanish cyber security cluster).

From evidence gathered in Trust-IT participation to “ClujIT Innovation Days” in March 2017, we see a great potential for WISER to be adopted by Romanian SMES which are ICT intensive and are currently lacking practical cybersecurity solutions.

Regarding AEI CITIC, it is one of the most active cybersecurity cluster in Europe. AEI CITIC is in contact with WISER to guarantee a WISER presence during the event “Encuentro Internacional de Seguridad de la Informacion (ENISE)” which is organized by INCIBE (Spanish National Cybersecurity Institute) and this would mean for WISER to gain great visibility to a large and very receptive audience.

Preference is given to Plan A although we believe that the plan B is also relevant for the WISER

objectives

In the definition of the final details for Plan A, WISER will also consider a solution which leads to delivering both option Plan A and Plan B.

Table 12 below provides events considered being suitable for promoting WISER and disseminating its results as it evolves over time. In some instances, concrete actions have already been identified, and details included.

Event Name	Date and location
Security of Things World	12-13 June 2017, Berlin
1 st CIPSEC workshop	14 June 2017, in Vilanova i La Geltrú, Barcelona, Spain
ATOS Technology Days	4-6 July 2017, Brussels
IEEE International Conference on Software Quality, Reliability & Security (QRS'17)	25-29 July 2017, Prague, http://paris.utdallas.edu/qrs17/
Information Security Network	11-12 September 2017, Reading
European Symposium on Research in Computer Security (ESORICS'17)	11-15 September 2017, Oslo, https://www.ntnu.edu/esorics2017
44CON	13-15 September 2017, London
Information Security Network	18 September 2017, London
Cybersecurity Week	25-29 September 2017, the Hague
World eID and Cybersecurity	25-27 September 2017, Marseille
Cybersecurity Nordic Conference	26-27 September 2017, Helsinki
Conference organized by XLAB	October or November 2017 – date still not fixed, Ljubljana, Slovenia
Cyber Threat Summit	24 October, Dublin

Table 12 - WISER Event Planner for last six months

4.5 Market Target 1 – Small Firms

4.5.1 Strategy and Expected Impact

Small- and medium sized enterprises (SMEs, or SMBs – small- and medium-sized businesses) are the backbone of the European economy. They are central to the Digital Single Market strategy as a means to revitalise the economy, by enabling all types of businesses to go digital and operate across borders more easily and cost effectively.

Strategy: Engage extensively with small- and medium-sized enterprises (SMEs/SMBs) as the backbone of the European economy. This group plays a central role in the European digital single market connecting over 500 million customers, helping to revitalise the economy by enabling all types of businesses to become digital and operate across borders more easily and cost effectively. WISER will allow SMEs to adopt a cyber-secure strategy at affordable costs. This group also represents an important source for rollout to other verticals.

The evolving small business landscape

Since the submission of D8.4, WISER has identified another important group of firms within the EU SME sector, namely Fintech companies (finance + technology). The DG CNECT Cloud Security Workshop (March 2016¹⁷) specifically called upon industry and research stakeholders to facilitate these small companies because they lack the very human and financial resources, and IT security expertise they need for an effective risk management at levels similar to larger Financial Service and Insurance counterparts.

The growing Fintech ecosystem is expected to continue building partnerships with banks and other financial institutions while extending its digital disruption into new categories like insurance¹⁸, making it a natural choice as a WISER target audience. WISER therefore has a clear role to play in facilitating the uptake of effective cyber risk management while helping to nourish a risk assessment culture across the business community.

Expected impact:

- Typical size: Estimated number of SMEs in the European Union: 23 million (99/100 businesses). 9 out of 10 companies are micros (less than 10 employees – 29%), whereas small firms with between 10 and 49 employees represent 21% and 17% have between 50 and 249 employees¹⁹. SMEs employ 2 in every 3 employees and on average produce 58 cents/euro. In recent years, they have helped create around 80% of new jobs.
- Bloodline for the EU economy: An increasing number of these businesses are becoming digital²⁰, prone to cyber risks, and therefore requiring even the most basic risk management tools. There are 4 million self-employed and micro businesses. This sector now accounts for 76% of all UK firms and contributes 10% of the Gross Domestic Product (GDP). This sector is the most exposed to sub-standard communication services and challenges presented by a lack of digital skills. Yet it stands to gain the most from the transformative effects of the internet²¹.
- Business priorities & IT skill sets: focusing on running business and acquiring new customers means they need ready-to-use tools for cyber risk management that are also within their small budgets. Because fewer than 20% of SMEs in Europe have an IT manager, tools and services should not require personnel with advanced IT skills.

WISER will help lower entry barriers to cyber security for small businesses, making it easier for them to build resilience in cyber space with user-friendly tools and services, at low cost and requiring few in-house resources to draw an effective cyber security strategy.

4.5.2 Messages, Channels and Formats

The WISER “Think Small – Think Secure” approach means tailoring messages, communication channels and formats in a way that lowers the barriers for small firms, as shown in the sample messaging below.

In the age of online business, the impact of a cyber breach can be huge and long lasting.

All businesses are at risk of a cyberattack, whether they are a Fortune 500 company, a family-run business, a utility company or a tech start-up.

Smaller businesses are being hit with seven million cyber attacks a year, which is costing

¹⁷ <https://ec.europa.eu/digital-single-market/en/news/cloud-security-workshop-building-trust-cloud-services-certification-and-beyond>.

¹⁸ <https://info.bbva.com/en/news/general/five-Fintech-trends-for-2016/>.

¹⁹ http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review/files/annual-report/infographics_en.pdf.

²⁰ http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review/files/annual-report/infographics_en.pdf.

²¹ According to the UK All-party Parliamentary Group for Information, Communication and Technology, ‘getting all micros online’ could generate €25bn to the national economy, <http://www.pictfor.org.uk/how-to-get-the-smallest-businesses-online/>.

the UK economy an astonishing £5.3 billion annually. Furthermore, they are more at risk of successful cyber attacks than larger companies as they often lack the budget and expertise to implement effective cybersecurity strategies. .

Your journey to cyber security starts with CyberWISER Light

Cyber security is most effective when integrated well with risk management that encompasses people, process, technology, policy and intelligence. Doing regular risk assessments and identifying vulnerabilities can definitely help SMEs to achieve cyber security fundamentals, however, many SMEs don't have financial resources, time and dedicated skills to dedicate to these activities.

CyberWISER Light can help overcome this gap by improving SMEs cyber risk management and detect vulnerabilities in their IT system without having to invest lots of time and resources. The assessment evaluates the risks and overall strength of an organisation's IT security. Most cyber criminals use existing critical flaws in infrastructure when they attack, so it is crucial to know where the vulnerabilities are.

WISER gives priority to formats that facilitate small companies in implementing an effective risk management strategy, considering also that many media and specialised channels cater to larger organisations. A sample of the formats used is provided in the table 13 below.

Media Platform	Cyber security essentials, practical tips and user-friendly guidelines. News on cyber risk landscape for SMEs. Section on relevant standards tailored to this target group. Event announcements relevant to this group.
Champion Packs (mostly from June 2016 on)	Specifically designed information packs (print and online) with statistics and quotes on how useful WISER is for SMEs, with the aim of building trust around the tools and encourage wide usage.
Twitter	Promoting relevant news and events published on the media platform; promotion of the WISER tools for SMEs. Business news of interest and funding, e.g. Innovate UK Cyber Security Vouchers. Examples: <i>Risk managers must work with #SMEs to promote healthy #riskmanagement along the value chain" #fermaforum</i> <i>UK businesses pushing for more #cybersecurity & #riskmanagement experts</i>
LinkedIn Group	Create and contribute to discussions on cyber security, risk management and cyber insurance, also asking small firms in our network about their top cyber security concerns and practices (and reporting them from f2f interactions). Share news and updates with peer projects. Share takeaway messages from events.
Newsletters	Launch of CyberWISER Light in May 2016: 1 newsletter every two months (May-June 2016), and then 1 newsletter every three months
Press releases	1 press release in English at the launch of CWL as part of the overall marketing campaign, potentially complemented by summaries in partner languages (target min: 3). Companies within the WISER network that operate critical infrastructures (e.g. energy, Fintech firms) will also receive the press release on the

	advanced mode.
Updated WISER Pilot marketing showcases	EAPs and FSPs are part of the communication plan as early adopters of WISER, e.g. providing quotes for press releases and content for blogs and tweets. ENERVALIS, 100% IT, Koofr, Wimedical, Marè Beachwear, Portic Barcelona

Table 13 - Updated Formats for engaging Small firms

WISER has identified an extended set of channels for reaching European SMEs, including mainstream press which is beginning to pay greater attention to cyber security (see Table 14).

Events	Innovate UK 2016, FSB Small Business Expo & National Conference 2016 (and similar local/national events in partner countries (e.g. business meet-ups and SME Days/Weeks), ICT2015 (mixed audiences).
SME media channels	Real Business, Business Insider, StartupNews, Business Matters, Tech City News, Business Zone
Sector specific media channels	The Fintech Times (@theFintechtimes), Fintech Finance, Fintech Forum
Business Multipliers and accelerators	EU: @UEAPME, @EBC_SMEs, @BITMi, @EUBIC, @EIT_Digital National: @austria_in_DK, @AgorianI, @AMETIC_es, @techUK, @austria_in_DK, @Pole_Systematic, @afrpc, @FranceClusters, @BITMi, @Irish_Biz, @isme_ie, @VNO_MKB_Brussel, @Swedishenterp, @EEN_vast, @cepyme_, @EEN_Wales, @innovateUK, @UKITA_UK, The Slovenian Business Club, GZS and Zitex (Slovenian Chamber of Commerce and Industry and export ICT firms). International: @ISBC_global, @INSME_, @AtosES Cyber security incubators: @CyLon
Fintech accelerators and companies	@FINTECHCircle, @FTInnovate, @FinLeap, @TLAFintech, @TechLondonAdv, @fdataUK (Financial Data and Technology Association) #FintechLondon, #FintechEvents
Standards for SMEs	CENELEC – the European Committee for electro-technical standards: @Standards4EU. Small Business Standards (the EU association representing SMEs): @sbs_sme, #Standards4SMEs. Cloud Security Alliance as a first entry point to cloud computing and cloud security (@cloudsa)

Table 14 - Updated sample of channels for reaching small firms

4.5.3 Actions and Targets for Small Firms – Last six months

WISER - Small Firms							
Actions	Main activities	Jun M25	July M26	Aug M27	Sept M28	Oct M29	Nov M30
Web Platform Updates	Content update on Cyberwiser.eu: - News & Events (also including Policy Guide) - MarketWatch - Best Practices - WISER products & services	x	x	x	x	x	x
	Newsletters		x			x	
Press & Media Campaign	WISER Flier					x	
	Roll up Banners/Posters					x	
	Interviews & Audio-visuals	x					
	Partner Promotional Kit	x				x	
	Infographs						
Social Media Activities	Press Release				x		
	Tweet sent	x	x	x	x	x	x
Other Community Building activities	LinkedIn post	x	x	x	x	x	x
	Face to face interaction						x
Dissemination of results	Synergies						
	Other activities						
	Presentations at events					x	
	Articles						
	Other activities						

Table 15 - Actions and Targets for Small Firms

4.6 Target Market 2 – Large Companies

4.6.1 Strategy and Expected Impact

Strategy: Engage with representatives from large companies across diverse sectors, encouraging the uptake of WISER tools and services, educating C-Suite executives on industry best practices and compliance with new EU regulations. This group also represents an important source for rollout to other verticals.

Specific targets include

- C-Level executives, especially chief information security officer (#CISO), chief information and technology officers (CIO/CTOs) that represent the main IT decision makers, but also chief executive and financial officers (CEO/CFOs) to encourage businesses to pursue a corporate approach (aka “joined-up” approach) to cyber security risk management across different market sectors.
- Industry influencers, experts on privacy and security, cloud service providers and owners of other critical infrastructures.

Expected impact: A widely recognised challenge for large company is the adoption of a holistic, boardroom approach to cyber risk management. Recent data shows that corporate directors are not sufficiently informed about cyber risks and incidents (FTSE Cyber Governance Health Check survey, KPMG, May 2016²²). Companies need to collaboratively work towards flexible and agile responses in an evolving threat landscape in order to reduce the likelihood of losing money, data and consumer confidence due to cyber-attacks.

Herein lies an important opportunity for WISER to rollout to market a complete suite of services that not only increase cyber resilience but also increase knowledge about the business impact of cyber incidents. While the CyberWISER Light service represents a possible initial step towards improved cyber risk management, this group can significantly benefit from the CyberWISER Essential and CyberWISER Plus.

4.6.2 Messages, Channels and Formats

Putting cyber-risk management at the very heart of good business practices

Cyber security is of critical importance to Europe’s large companies running complex IT systems and critical infrastructures. Millions of Euros are lost to cyber-crime each year and online security is a growing concern for businesses, with attacks increasing against large corporate businesses and critical infrastructures.

WISER value proposition

Anticipating, identifying and reducing threats by embedding cyber security risk management into business processes and assessing direct and indirect impact.

Examples of core messages targeting large companies are provided in the box below.

A company-wide Cyber Risk Management

A cyber attack often interrupts business continuity and erodes customers’ trust and business reputation.

Yet many companies, large and small, fail to see that a cyber risk is a business risk.

²² http://www.computerweekly.com/news/450295785/Two-thirds-of-UK-businesses-hit-by-cyber-security-breaches-but-directors-remain-unaware?utm_medium=EM&asrc=EM_EDA_56792139&utm_campaign=20160509_Two-thirds%20of%20UK%20businesses%20hit%20by%20cyber%20security%20breaches,%20but%20directors%20remain%20unaware_&utm_source=EDA.

Today's fast-evolving threat landscape calls for a company-wide approach to cyber risk management. This is where WISER advanced services come into play.

The services provide both quantitative and qualitative data, enabling service users to align information about security alerts with key business decisions helping to reduce gap between executive and IT personnel.

The WISER novel approach allows company executives, CEOs, CFOs, and IT managers to work together on a company wide risk management strategy that can evolve with the threat landscape.

WISER uses a range of different formats to engage with large companies (see Table 16), including position papers offering industry insights into key challenges and recommendations to foster industry-wide best practices.

Media Platform	Cyber security C-Suite Guide to Cyber Security. News on cyber risk landscape for big companies and across different sectors. Section on best practices and the importance of standards, including updates and insights from experts recruited by WISER. Event announcements relevant to this group, including information on how to connect and benefit.
Twitter	Promoting relevant news and events published on the media platform; promotion of the WISER tools and practical guides.
LinkedIn Group	Create and contribute to discussions on cyber security, risk management and cyber insurance, also asking large companies in our network about their top cyber security concerns and practices (and reporting them from f2f interactions). Share news and updates with peer projects. Share takeaway messages from events.
Newsletters	1 newsletter every three months, starting in June 2016.
Press releases	1 press release on the launch of the tool for advanced mode of operation as part of the larger marketing campaign. Other press releases will be produced and distributed on a case by case basis.
Policy Guides and Best Practice market watch	Guides to new EU regulations hosted on the WISER media platform. An updated market watch on industry best practices on both cyber security and implementation of policy priorities. Best practices also include contributions to national cyber security strategies and corporate strategies enabling the digitisation/transformation of traditional vertical markets.
Pilot marketing showcase	The EAPs and FSPs can support WISER communications and marketing with quotes and contributions to blogs and tweets. Aon, Rexel, OTG (oil tech group), Tunstall

Table 16 - Updated Formats for engaging Large Companies

WISER uses a diverse set of channels to reach out to large companies (see Table 17). With regard to media channels, it is important to note that many IT and specialised channels cover topics related to WISER which is not often the case in channels targeting smaller organisations.

Events	EuroCACS, Security IT Summit, InfoSecurity Europe, Datacloud 2016, International Risk Management Conference, The Security Culture Conference 2016 + CSA Nordic Summit, OTS conference, FERMA European Risk Seminar (RM Forum pending), CSA EMEA Congress 2016
---------------	---

IT Media channels	Computer Weekly, Tech Target & Search Security, Business Cloud News, Cloud Computing Intelligence Magazine, Cloud Pro weekly newsletter, Security Info Watch, Threat Post, CIO, Cyber Defense Magazine, CSO Online
Sector specific media channels	Business Insurance, Captive Insurance Times, Catastrophe Risk Management, Commercial Risk Europe, Continuity, Insurance & Risk, Global Trade Review, Insurance Insider/Inside FAC/Trading Risk, Insurance Times
Business Multipliers (sample)	Big Data Value Association (BDVA – Atos is a founding member), EIT Digital (industry members), EuroCloud (also for SMEs), EuroCIOs
Standards Bodies	International Standardisation Organisation (ISO), IEEE Cloud (@ieeeccloud), Cloud Security Alliance (@cloudsa)

Table 17 - Updated Channels for targeting Large Companies

4.6.3 Actions and Targets for Large companies – Last six months

WISER - Large Companies							
Actions	Main activities	Jun M25	July M26	Aug M27	Sept M28	Oct M29	Nov M30
Web Platform Updates	Content update on Cyberwiser.eu: - News & Events (also including Policy Guide) - MarketWatch - Best Practices - WISER products & services	x	x	x	x	x	x
	Newsletters	x				x	
Press & Media Campaign	WISER Flier					x	
	Roll up Banners/Posters					x	
	Interviews & Audio-visuals	x					
	Partner Promotional Kit	x					
	Infographs						
	Press Release				x		
Social Media Activities	Tweet sent	x	x	x	x	x	x
	LinkedIn post	x	x	x	x	x	x
Other Community Building activities	Face to face interaction						x
	Synergies						
	Other activities						
Dissemination of results	Presentations at events					x	
	Articles						
	Other activities						

Table 18 - Actions and Targets for Large companies

4.7 Target Market 3 – Public Sector

4.7.1 Strategy and Expected Impact

Strategy: Provide tools and services to help public sector organisations improve cyber resilience in the face of new threats. Educate public sector organisations on new cyber threats affecting them and engage with representatives from this target group through the relevant EAPs, scientific media channels and events.

Through Task 8.5 (Socio-economic impact tool development), WISER seeks practical responses to the impacts of cyber incidents by helping SMEs and small teams in public administration assess the likely effects of a cyber incident from an economic and sociological perspective. To achieve this goal, WISER has developed a Socio-economic Impact Assessment Tool (CW-SEIT).

Expected impact:

WISER has dedicated effort in lowering the entry barrier to cyber risk management for SMEs and small IT teams in the public sector. The aim is to demonstrate that cyber security does not have to be excessively time consuming or complex. Several new tools follow the WISER “light” approach, such as CyberWISER Light and the Socio-economic Impact Assessment Tool, in enabling SMEs and small IT teams within public administration who are not IT or cyber-savvy to overcome time and financial constraints.

4.7.2 Messages, Channels and Formats

The WISER messaging for the public sector caters for both small and large organisations. Sample messages are provided in the boxes below.

Consolidating a proactive approach to cyber security

Cybersecurity is becoming an increasingly common topic of conversation across the public sector, and for good reason. Although high-profile cases like last year’s cyberattacks on Lukas Hospital in Neuss, Germany and the WannaCry Ransomware Attack in May 2017 dominate headlines, cyberthreats are presenting a serious and growing risk to all government organizations at all levels.

State and local governments need to start doing more to mitigate cybersecurity risks, and should have a response plan ready in case a breach does occur.

Because state and local governments have less to spend on security teams, however, the key is making smart investments in personnel and technology.

An essential part of the WISER mission is to provide dedicated tools that are usable and useful especially to small organisations (e.g. SMEs and small IT teams in public administration) lacking the skills and means for efficient risk management but facing a variety of potential impacts.

Such an approach responds well to key findings reported in the UK Cyber Security Strategy 2016-2021 (November 2016) support the WISER “light” approach for small businesses and IT teams. It is important to note that the strategy highlights the currently low market uptake of cyber security tools and products, which is symptomatic of an incorrect approach to cyber risk management. Earlier, in May 2016 a UK government-led report on business practices underscored the importance of training staff on cyber security, with particular reference to SMEs, where the currently low levels of cyber risk management could have significant impact on small businesses and IT teams within

public administration.

WISER uses different formats to engage with and reach out to the public sector, especially IT decision makers (See Table 19 & 20).

Media Platform	Cyber security essentials, practical tips and user-friendly guidelines. News on cyber risk landscape for the public sector. Section on relevant standards and EU regulations tailored to this target group. Event announcements relevant to this group.
Twitter	Promoting relevant news and events published on the media platform; promotion of the WISER tools for this target group. Public surveys of interest. Dialogues with EU initiatives, e.g. EU_eGov.
LinkedIn Group	Join relevant groups to share best practices and the relevant WISER tools, FAQs and scanning of specific concerns.
Newsletters	Launch of non-invasive tool: 1 newsletter every three months (Jan – May 2016), and then 1 newsletter every six months.
Press releases	1 press release at the launch of each tool (basic and advanced mode).
Champion Packs	An information pack with statistics on cyber risks and on the benefits of WISER for the public sector. As the project progresses, these packs will include the WISER showcase.
Standards Bodies	Cloud Security Alliance as a first entry point (@cloudsa). OASIS (@OASISopen)
Pilot Showcases	EBI (European Bioinformatics institute), FMI (Friedrich Miescher institute), PSCN

Table 19 – Updated Formats for engaging the Public Sector

Events	European conferences and summits organised by the Cloud Security Alliance and OASIS. At least one annual eGovernment event.
Scientific channels	Science Node, Government Computing, Public Tech, Government Procurement

Table 20 - Updated Channels for engaging the Public Sector

4.7.3 Actions and Targets for Public Sector – Last six months

WISER - Public Sector							
Actions	Main activities	Jun M25	July M26	Aug M27	Sept M28	Oct M29	Nov M30
Web Platform Updates	Content update on Cyberwiser.eu: - News & Events (also including Policy Guide) - MarketWatch - Best Practices - WISER products & services	x	x	x	x	x	x
	Newsletters				x	x	
Press & Media Campaign	WISER Flier					x	
	Roll up Banners/Posters					x	
	Interviews & Audio-visuals	x					
	Partner Promotional Kit	x			x		
	Infographs						
Social Media Activities	Press Release				x		
	Tweet sent	x	x	x	x	x	x
Other Community Building activities	LinkedIn post	x	x	x	x	x	x
	Face to face interaction						x
	Synergies						
Dissemination of results	Other activities						
	Presentations at events					x	
	Articles						x
	Other activities						

Table 21 - Actions and Targets for Public Sector

4.8 Market Target 4 – Policy Stakeholders in EU and Internationally

4.8.1 Strategy and Expected Impact

The revised strategy since D8.5 is the result of year one engagement with public and private sector stakeholders, highlighting challenges around the implementation of new EU regulations and the need to improve knowledge sharing on cyber security best practices across different market sectors²³.

WISER will now adopt a 3-tier approach to its engagement with policy stakeholders in EU and internationally:

1. Sharing insights on new EU regulations (e.g. NISD, DPRR) and engaging with centres of expertise for cyber security in Europe (e.g. ENISA), drawing also on the Cartography of National Cyber Security Strategies (WISER D6.9, July 2016).

ENISA, the EU Agency for Network and Information Security and centre of excellence for cyber security, is a key stakeholder for WISER. ENISA not only hosts an interactive map on national cyber security strategies, it also plays a key role in coordinating the strategy group with member state representatives. Another ENISA group looks at operational aspects, such as Computer Emergency Readiness Teams (CERTs).

2. Establishing synergies with EU-funded R&I actions and sharing WISER advances with the technical community (e.g. projects funded under Unit Trust and Security and the Cluster on Data Protection, Security and Privacy (DPSP) under Unit Software, Services, Cloud).
3. Engaging with international initiatives on cyber security and relevant standards organisations (e.g. NIST).

WISER Strategy: Establish synergies with relevant EU and international initiatives to share information and best practices in the industry and respective policy contexts, on scaling the incentives for businesses and training for engagement and raising awareness.

In particular, WISER liaises with a number of European Initiatives, operating in the field of ICT innovation and in other fields, that might present complementary approaches and objectives. Contact with the following several European Initiatives such as WITDOM and PRISMACloud have already been established (as part of the ICT 2015 event), and will be further expanded in the lifetime of the present communication plan.

Expected impact: The collection of case studies will help provide concrete examples of best practices for promotion across respective web and social platforms, thus increasing visibility. More generally, WISER contributes to trust and security as key pillars of the Digital Single Market, in that the project will help to:

- Strengthen the EU cyber security industry and make sure European citizens and businesses have access to more innovative, secure and user-friendly solutions that take into account European rules and values (Pillar I).
- Ensure a level playing field for all types of organisations, especially small firms by lowering the entry barrier to cyber risk management (Pillar II).

Relation to other WISER activities: WP6 “Pilots” includes a contribution to NIS activities by creating public-private sector synergies to share information and best practices on risk management practices, drawing on the pilot experiences and insurance expertise in EU and globally, especially the U.S.”, mostly to be achieved through *Task 6.5* “Synergies and international liaison on best practices”, led by Trust-IT and with involvement of other WISER partners.

²³ Cloud Security Workshop March 2016, op cit.

4.8.2 Messages, Formats and Channels

Cyber space is the backbone of the digital society and key to economic growth but Europe needs effective security mechanisms underpinning its digital single market. The Network and Information Security Directive (NISD) is a new EU regulations bringing new obligations to EU member states and certain types of organisations operating within and across them to build capabilities against cyber risks.

POLICY GUIDE – AN INTRODUCTION TO THE NETWORK AND INFORMATION SECURITY DIRECTIVE (NISD)

Role of EU Member States in building national cyber security capabilities

Sectors important to the European economy are undergoing considerable digital transformation while at the same time facing unprecedented vulnerabilities. Critical infrastructures, such as energy, health, water and transport systems, risk major service disruptions. Another concern is the increasing interdependency between these infrastructures, further increasing vulnerabilities, for example, electric vehicles connected to the smart grid.

The European Union member states need to establish a minimum level of common capabilities for cyber security, including beyond national borders. It is also important that each member state has a good level of awareness of industry risks and takes appropriate steps for risk management, especially for their critical infrastructures, reporting on any cyber-attacks they are subjected to. In this respect, qualified response teams are particularly important.

Under the Network and Information Security Directive (NISD), member states are required to put in place a minimum set of capabilities at national level as part of their cyber security strategy, that is C-CERT and experts in information and networking security. Furthermore, member states are to ensure that operators of essential services and digital service providers adopt security requirements²⁴.

WISER uses the following formats and channels to engage with stakeholders related to policy priorities for a secure Digital Single Market, including new research and innovation initiatives (see Table 22 and 23).

Media Platform	Policy briefs on the state of play of national cyber security strategies and best practices. Informing this group about standards advancements and global co-operation in the area. Briefs on the impact of WISER.
Twitter	Promoting policy and standards-related news and events and updates from the digital agenda twitter account (@DigitalAgendaEU).
LinkedIn Group	Share relevant digital agenda blogs ²⁵ and policy updates.
Newsletters	1 annual newsletter.
Press releases	1 press release at project end.

Table 22 – Updated Formats for engaging with Policy Stakeholders

²⁴ Pierre Chatanet, Deputy Head of Unit Trust & Security, DG CNECT, Cloud Security Workshop, op cit.).

²⁵ https://ec.europa.eu/digital-agenda/blog_home/.

Events	European conferences and summits organised by the Cloud Security Alliance ²⁶ and OASIS.
Policy channels	@DSMeu, @EU_TrustSec, @EU_Commission

Table 23 - Updated Channels for reaching Policy Stakeholders

²⁶ <http://csa-cee-summit.eu/>.

4.8.3 Actions and Targets for Policy & Standard Bodies – Last six months

WISER - Policy & Standard Bodies							
Actions	Main activities	Jun M25	July M26	Aug M27	Sept M28	Oct M29	Nov M30
Web Platform Updates	Content update on Cyberwiser.eu: - News & Events (also including Policy Guide) - MarketWatch - Best Practices - WISER products & services	x	x	x	x	x	x
	Newsletters					x	
Press & Media Campaign	WISER Flier					x	
	Roll up Banners/Posters					x	
	Interviews & Audio-visuals	x					
	Partner Promotional Kit	x					
	Infographs						
Social Media Activities	Press Release				x		
	Tweet sent	x	x	x	x	x	x
Other Community Building activities	LinkedIN post	x	x	x	x	x	x
	Face to face interaction						x
Dissemination of results	Synergies						
	Other activities						
	Presentations at events					x	
	Articles						
	Other activities						

Table 24 - Actions and Targets for Policy & Standard Bodies

4.9 Market Target 5 – General Public

4.9.1 Strategy and Expected Impact

Today, most of our lives, from communication to commerce, fundamentally depend on the Internet. The cyber security issues that result challenge almost everyone but most of all they affect individuals. Individuals face new threats to their online and mobile devices, privacy and money, either directly or indirectly through cyber attacks on service providers.

European citizens therefore have to know and trust that the systems underpinning digital services are safe and secure and have to be properly educated about how to protect themselves online. Despite the increasingly public nature of cyber attacks on people and businesses, still majority of European citizens and employees are lacking skills to tackle cyber risks.

Strategy: in the mid-term, deliver up to speed security messages, explaining implications for European citizens and best practices easier to follow.

Expected Impact: Creating a culture of cyber awareness across all sectors of society with practical advice on defending individuals from cyber risks.

4.9.2 Messages, Formats and Channels

Cyber Security – What every citizen needs to know

Hackers can use your email to gain access to all your personal accounts, leaving you vulnerable to identity theft or fraud.

Make your passwords stronger with three random words

To create a strong password simply choose three random words. Numbers and symbols can still be used if needed, however, using three random words is the key to creating a strong password.

Your most important accounts are your email and online banking. With access to your email, hackers can take control of all your online accounts, by asking for the password to be reset, and use the information your email contains can easily be pieced together to create a profile of your identity.

WISER will use a core set of formats and channels to reach out to the general public and help make them cyber wiser (see Table 25).

Media Platform	Practical guides to protecting personal data online, including banking and commercial transactions, and social networking. Items educating citizens on what their national governments are doing to increase cyber security capabilities and service provider best practices.
Online forums	@EUWatchers (EUwatch Info Hub - European Citizen Information Network Hub); @EU_eGov (European Commission, CONNECT 'Public Services' Unit, working on Cross Border Digital Public Services (eGovernment) and ICT-enabled Public Sector Innovation), @DigitalAgendaEU.
Press releases	1 press release
Media Channels	National newspapers in partner countries. UK examples include: BBC, Daily Telegraph, The Independent, The Times and Sunday Times

Table 25 - Channels and Formats for engaging with General Public

5 Last six months Roadmap (June 2017 – November 2017)

In table 26 below we summarize the actions already mentioned in sections 4.4 to have a complete picture of the activities that will be carried out based on the WISER Market Targets.

	WISER Targets						
Market Target 1	Small Firms						
Market Target 2	Large Corporations						
Market Target 3	Public Sector						
Market Target 4	Policy and Standard bodies						
Market Target 5	General public						
All Market Targets	All Targets						
WISER - Roadmap							
Actions	Main activities	Jun M25	July M26	Aug M27	Sept M28	Oct M29	Nov M30
Web Platform Updates	Content update on Cyberwiser.eu: - News & Events (also including Policy Guide) - MarketWatch - Best Practices - WISER products & services	x	x	x	x	x	x
	Newsletters		x			x	
Press & Media Campaign	WISER Flier					x	
	Roll up Banners/Posters					x	
	Interviews & Audio-visuals	x					
	Partner Promotional Kit	x				x	
	Infographs						
	Press Release				x		
Social Media Activities	Tweet sent	x	x	x	x	x	x
	LinkedIn post	x	x	x	x	x	x
Other Community Building activities	Face to face interaction						x
	Synergies						
	Other activities						
Dissemination of results	Presentations at events					x	
	Articles						x
	Other activities						

Table 26 - Last six months Roadmap

6 Conclusions

D8.6 “Communication Plan, Final Version” serves two main purposes:

- It reports on the activities performed in the first 24 months of WISER with particular reference to the period May 2016 to May 2017.

-
- It provides plans for the last 6 months of WISER, that is, June 2017 (M25) to November 2017 (M30).

The main conclusions of D8.6 “Communication Plan, Final Version” are:

- Regarding cybersecurity, there is still very little awareness amongst small digital businesses as well as individuals across Europe. WISER will make a difference in this respect through the development and rollout of a new CW-SEIT tool that offers practical advice and checklists on cyber risk management in a business friendly way. It is an example of how WISER looks at cybersecurity through a business lens.
- The strategic goals for the 6 month sprint are to boost the use of the CyberWISER service packages now that the full range is available as aligned with D2.6. Using three pillars (full product range, business model, portability to other verticals) WISER aims to increase the KPIs that are currently below initial expectation. To this end, WISER Partners are committed to the 6 month plan.
- WISER stakeholder engagement is wide-ranging to include all the informative material produced in multiple languages, connections with national business associations and cybersecurity Clusters as well as risk management professionals. The new insights gained through D8.3 also give WISER a competitive edge in terms of expertise that is vital for helping European businesses become cyber secure also in view of the GDPR.

7 Annex 1 – Complete List of Media Channels Targeted

The table below lists following media and press channels are sourced from the partner networks and will be selected over the lifetime of the project for press campaigns.

IT and Security Media	
Computer Weekly, Tech Target & Search Security http://www.computerweekly.com/ http://www.techtarget.com/	CW: covers issues, challenges and trends facing today's IT leaders with a subscription of 200,000. TT targets technology buyers researching and making technology decisions, and provides a weekly information security/cyber security update.
Business Cloud News www.businesscloudnews.com/	News and analysis for the global cloud computing industry and enterprise IT professionals
Cloud Computing Intelligence Magazine www.cloudcomputingintelligence.com/	Cloud service news and business processes targeting UK professionals (IT and businesses).
Cloud Pro weekly newsletter www.itpro.co.uk/	News and reports for business and IT decision makers.
Computer World (security section) http://www.computerworld.com/ http://www.cw.no/ (Norwegian Computerworld)	Security news, trends, analysis and practical advice for decision makers and influencers.
Global Security Mag https://www.globalsecuritymag.com/	News, features, online version and magazine
TechWeekEurope UK http://www.techweekeurope.co.uk/	News, features, reviews of business technology for IT decision makers.
Security Info Watch http://www.securityinfowatch.com/magazine/stec/issue/2015/sep	Business cases for purchasing and implementing IT and services for leading executives.
Security Week www.securityweek.com	Malware and threats, cybercrime, risk and compliance, security architecture.
Threat Post http://threatpost.com/	The news site of the Kaspersky Lab with a focus on IT and business security for global audiences.
The Register www.theregister.co.uk	Online tech channel with audiences mostly from the UK and US, but also Canada, Australia and northern Europe.
IT Briefcase www.itbriefcase.net	IT professionals researching software solutions, including open source.
CIO www.cio.com	Targets chief information officers and IT leaders with relevant technology news and features.

Cyber Defense Magazine www.cyberdefensemagazine.com	IT security professionals covering products and services in ICT.
SC Magazine www.scmagazine.com/	Targeting IT security professionals on business and technical information about security challenges.
Info Security www.infosecurity-magazine.com	Coverage on the IT security industry, including opinion pieces from industry experts.
CSO Online www.csoonline.com/	News, analysis and research on security and risk management topics, including IT security, business continuity, identity and access management, loss prevention.
Sector specific – financial and insurance services	
Business Insurance http://www.businessinsurance.com/	Managers, insurers, brokers and other providers of insurance products and services.
Captive Insurance Times http://www.captiveinsurancetimes.com	Global insurance markets and professionals.
Catastrophe Risk Management http://www.cii.co.uk/about/about-the-cii/the-journal/	Official membership magazine of the Chartered Insurance Institute reaches 79,000 professionals within the insurance industry.
Commercial Risk Europe http://www.commercialriskeurope.com/	Pan-European newspaper dedicated to news, trends and issues critical to corporate risk and insurance management executives across Europe.
Continuity, Insurance & Risk http://www.cirmagazine.com/	Risk management, business continuity and commercial insurance purchasers
Global Trade Review http://www.gtreview.com/	News source, publisher and event organiser for the global trade, commodity, export and supply chain finance industries.
Insurance Day https://www.insuranceday.com/	Business decision makers in the international insurance community.
Insurance Insider/Inside FAC/Trading Risk http://www.insuranceinsider.com/ http://www.insidefac.com/about-us http://www.insuranceinsider.com/trading-risk	Professionals with an interest in the London and international insurance markets.
Insurance ERM – Enterprise Risk Management https://www.insuranceerm.com/	Enterprise risk management, Solvency II, capital planning, asset/liability management, risk governance, actuarial systems, software, regulation and supervision to market risks, investment risk, longevity risk, operational risk and catastrophe risk.
Insurance Services Network https://irletter.com/isn/	International insurance professionals worldwide, with an international community of

	brokers, underwriters and risk managers.
Insurance Times http://www.insurancetimes.co.uk/	Insurance in the UK for decision-makers, business placers and principals in brokers, insurers and service suppliers.
Intelligent Insurer http://www.intelligentinsurer.com/	Buyers, capital providers and brokers of reinsurance and wholesale insurance.
Financial Director http://www.financialdirector.co.uk/	Finance, regulation, legal, procurement, public sector.
Risk Management Professional http://www.rmprofessional.com/	Quarterly title for risk managers and enterprise risk, with a print circulation of over 5,500.
Strategic Risk http://www.strategic-risk-global.com/	Risk and corporate governance news and insight to national, regional and multinational corporations across Europe, Middle East, and Asia.
The Actuary http://www.theactuary.com/	Targets actuarial profession in the UK, including advertising and reporting vacancies within the profession.
Fintech	
The Fintech Times http://theFintechtimes.com/@theFintechtimes	Online media and monthly newsletter covering the fast-paced Fintech space. Targets company directors, entrepreneurs, managers and business-minded people. People in finance, banking, investment, tech and start-ups.
Financial IT www.financialit.net	Cutting edge financial technology magazine, covering the latest trends and issues in banking, payments & cash management, securities services.
Fintech Finance http://www.Fintech.finance/	Provides key decision-makers globally within the foremost financial services organisations with consistent and accurate intelligence on emerging trends, breakthrough technologies and stimulating developments, helping them to make informed decisions.
Fintech Forum	Largest hub for Fintech in Europe with a mission to build the financial services of the future, working with a global network, online presence, events, studies and advisory services.
Mainstream Press	
BBC (including News Planning and Online News) http://www.bbc.com/	National and international news, including business and technology reports.

Bloomberg http://www.bloomberg.com/europe	Financial news, data, analysis.
CFO Magazine http://ww2.cfo.com/	Markets, growth companies, banking and capitals, risk compliance.
City AM http://www.cityam.com/	Financial and business news with a daily readership of 399,000 professionals, including newspaper distribution in London and other areas of high business concentration.
Dow Jones http://www.dowjones.com/	Business and finance news. Risk and compliance. Research and insights.
The Economist http://www.economist.com/	Authoritative insights and opinion on international business, finance, IT, politics and the connections between them.
Evening Standard (UK) http://www.standard.co.uk/	Daily newspaper, which also covers business news.
Daily Telegraph (UK national) & Sunday Telegraph http://www.telegraph.co.uk/	Daily newspaper, which also covers business and technology news. The Sunday edition also periodically includes IT and cloud coverage from business experts.
Financial Times http://www.ft.com/home/europe	UK and international business, finance, economic and political news.
The Independent (UK) http://www.independent.co.uk/	Daily international coverage including business and technology. Its reports have included the EU cloud computing strategy and policy.
Reuters http://www.reuters.com/news/world	Business, markets, and technology.
The Times & Sunday Times http://www.thetimes.co.uk/tto/news/ http://www.thesundaytimes.co.uk/sto/	Daily and Sunday edition that also covers business and technology. Its Sunday supplements have also covered cloud computing, and IT security.
Sunday Express http://www.express.co.uk/news/	Daily national, also covers finance.
AMI Media Planner http://www.media-planner.co.uk/Static/index.aspx	A research and planning service for communications and PR activities across the press, news and broadcast programming.
Channels for the public sector	
Join-up Europe https://joinup.ec.europa.eu	Services that aim to help e-Government professionals share their experience with each other.
Science Node https://sciencenode.org/	Online, free publication on advanced computing, research networks and tech trends.
ASCENT blog	Website of scientific community of ATOS.

ASCENT Journey

Annual extensive studies providing insight to future technology trends and can use technology to grow and transform.

8 Annex 2 Sample of communication material

I WISER Marketing Package – CyberWISER Light CyberWISER Essential, CyberWISER Plus postcards



CyberWISER Plus: online package and onsite services for company-wide cyber risk management

In an increasingly connected world, cyberattacks can have a huge and long-lasting impact on organisations of any size. Risks include multi-channel threats from the same location or simultaneous attacks on a single access point from multiple locations across the globe, causing business interruption or a data breach.

Every digital business is at risk, from financial institutions and research firms to retailers and utility providers. Cyber risks are business risks that have both direct economic impacts but also indirect effects on a company's reputation and customer trust.

A company-wide Cyber Risk Management

Traditional risk assessment processes can take days to provide results and are not fit for today's fast-evolving cyber threat landscape. With **CyberWISER Plus** companies can detect, monitor and manage in real time vulnerabilities in their IT system.

CyberWISER Plus comes with an onsite support service, where the **CyberWISER** team of experts steps in to devise a company-wide approach to cyber risk management and takes care of installing the service package.

TAKE ACTION TODAY - Connect with CyberWISER

- www.cyberwiser.eu - register as a user
- @cyberwiser
- https://bit.ly/2d8a111/
- cyberwiser@chweidder.com - sign up for our newsletter

CyberWISER Essential: Cyber Threat Detection and Monitoring in real time

Connected world: A fast-evolving risk landscape

The growing number of connected devices and people is bringing many business benefits and opportunities, but also an increasing number of cyberattacks with direct economic losses and indirect effects, such as reputational damage. Yet, many companies, large and small, fail to see that a cyber risk is a business risk. Today's fast-evolving threat landscape calls for a company-wide approach to cyber risk management, it also calls for cyber security service packages that can react quickly and enable companies to make an informed decision about mitigation actions.

CyberWISER Essential – Real-time risk management

- **CyberWISER Essential** helps SMEs and larger companies counter the threat of cyberattacks.
- Companies can detect, monitor and assess their IT vulnerabilities in real time. This means organisations can now turn threat intelligence into business decision-making actions.
- **Real Time Risk Assessment** helps detect vulnerabilities in the IT system with valuable insights about indirect impact of a cyberattack.
- User-friendly Dashboard with analytical features showing risk graphs and trends for continuous monitoring.
- Decision Support System with built-in mitigation measures based on recognised international best practices in WISER expertise.

TAKE ACTION TODAY - Connect with CyberWISER

- www.cyberwiser.eu - register as a user
- @cyberwiser
- https://bit.ly/2d8a111/
- cyberwiser@chweidder.com - sign up for our newsletter

CyberWISER Plus: online package and onsite services for company-wide cyber risk management

In an increasingly connected world, cyberattacks can have a huge and long-lasting impact on organisations of any size. Risks include multi-channel threats from the same location or simultaneous attacks on a single access point from multiple locations across the globe, causing business interruption or a data breach.

Every digital business is at risk, from financial institutions and research firms to retailers and utility providers. Cyber risks are business risks that have both direct economic impacts but also indirect effects on a company's reputation and customer trust.

A company-wide Cyber Risk Management

Traditional risk assessment processes can take days to provide results and are not fit for today's fast-evolving cyber threat landscape. With **CyberWISER Plus** companies can detect, monitor and manage in real time vulnerabilities in their IT system.

CyberWISER Plus comes with an onsite support service, where the **CyberWISER** team of experts steps in to devise a company-wide approach to cyber risk management and takes care of installing the service package.

TAKE ACTION TODAY - Connect with CyberWISER

- www.cyberwiser.eu - register as a user
- @cyberwiser
- https://bit.ly/2d8a111/
- cyberwiser@chweidder.com - sign up for our newsletter

Service package features

- **Real Time Monitoring and Real Time Risk Assessment:** a cost-benefit analysis and an assessment of indirect impacts based on your risk profile.
- **Dashboard:** crucial at-a-glance information about cyber risks, vulnerabilities and incidents detected, helping you track real risks.
- **Decision Support System:** Cost-benefit analysis comparing and ranking different mitigation measures that can be taken against cyber threats.
- **WISER Online and Onsite Service Support** from a team of cybersecurity experts.

Testimonials

"The level of sophistication of cyberattacks is increasing with at least three different ways of using the cyber weapon: cyber sabotage, cyber data theft and cyber tampering of funds. WISER's real-time risk assessment can quickly identify risk factors. This drastically reduces events that are high impact to business in the financial sector. CyberWISER Essential and Plus are helping us moving towards preventative measures to deal with cyber-crime". **Samira Ceballos, Aon**

"The integrated approach to control mitigating activities will address cyber security threats and their consequences in critical information infrastructure. This novel approach will empower decision makers in the public and private sectors to assess cyber risks and their impacts effectively". **Antonia Alvarez, Aon**

Improve your cyber risk management today with CyberWISER ESSENTIAL: www.cyberwiser.eu

The WISER novel approach allows company executives, CEOs, CFOs, and IT managers to work together on a company-wide risk management strategy that can evolve with the threat landscape.

Testimonials

"Working with WISER helped us a lot to increase the security awareness in our company. The monitoring framework makes you realise that there are indeed serious weaknesses out there attempting to hack your network every day. You can trace these attempts through the system log files and take appropriate countermeasures. The system works as an early warning. In the test period, we asked an external company to try and hack our system, we could follow what they were doing every step of the way". **San Basilemberto, ENERVALS**

"The cyber risk management functionalities of CyberWISER Essential and Plus provide an additional layer of security management and decision making capabilities currently not available. This will provide value for our business in the existing energy products and services sector". **Roberto Marcella, Chief Information Security Officer at REXEL**

Service package features

- **Real Time Monitoring and Real Time Risk Assessment:** a cost-benefit analysis and an assessment of indirect impacts based on your risk profile.
- **Dashboard:** crucial at-a-glance information about cyber risks, vulnerabilities and incidents detected, helping you track real risks.
- **Decision Support System:** Cost-benefit analysis comparing and ranking different mitigation measures that can be taken against cyber threats.
- **WISER Online and Onsite Service Support** from a team of cybersecurity experts.

Testimonials

"The level of sophistication of cyberattacks is increasing with at least three different ways of using the cyber weapon: cyber sabotage, cyber data theft and cyber tampering of funds. WISER's real-time risk assessment can quickly identify risk factors. This drastically reduces events that are high impact to business in the financial sector. CyberWISER Essential and Plus are helping us moving towards preventative measures to deal with cyber-crime". **Samira Ceballos, Aon**

"The integrated approach to control mitigating activities will address cyber security threats and their consequences in critical information infrastructure. This novel approach will empower decision makers in the public and private sectors to assess cyber risks and their impacts effectively". **Antonia Alvarez, Aon**

II Logos design for PR circulation



CYBERWISER LIGHT

CYBERWISER ESSENTIAL

CYBERWISER PLUS

CYBERWISER CARTOGRAPHY

CYBERWISER SEIT

AtoS

Aon

Enervalis

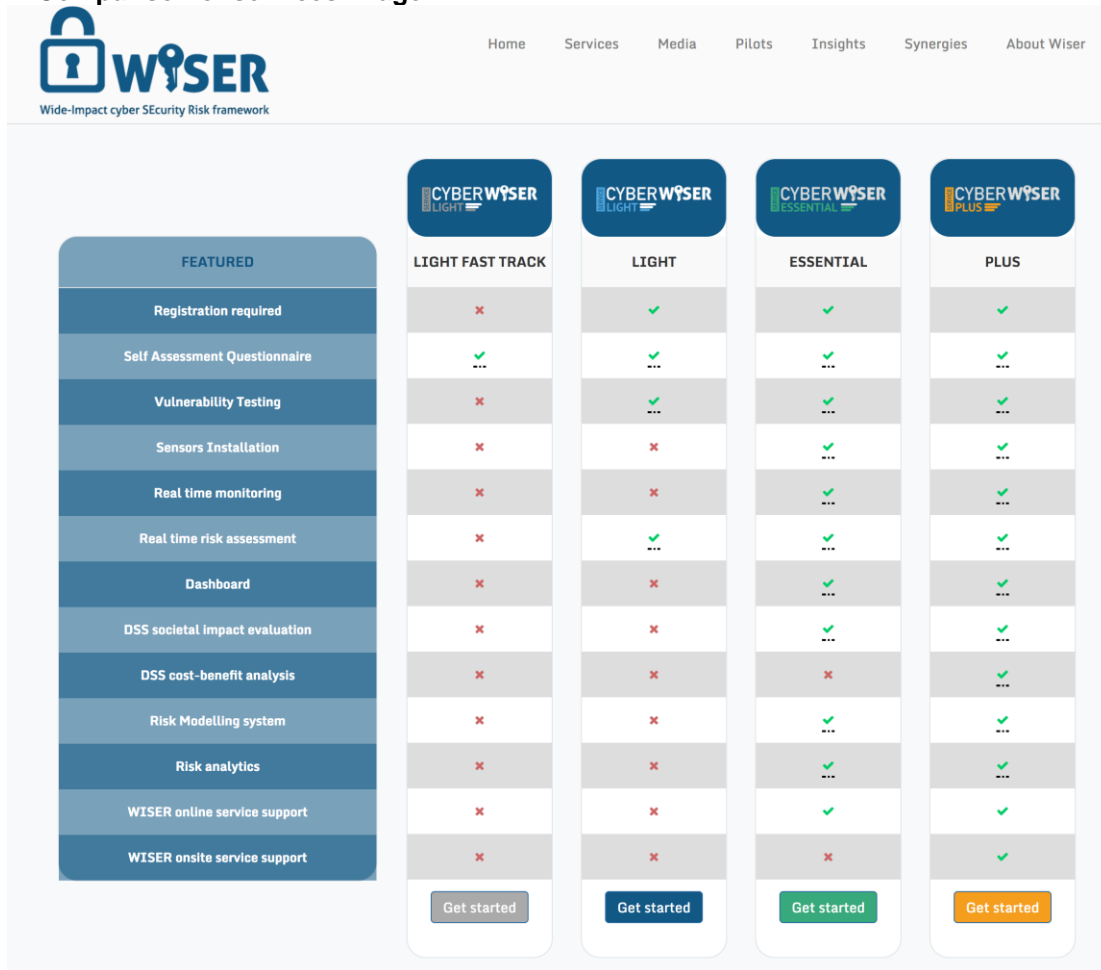
REXEL
a world of energy

SINTEF

Trust-IT Services
Communicating ICT to markets

XLAB
NOT IDLE

III Comparison of services image



	CYBERWISER LIGHT FAST TRACK	CYBERWISER LIGHT	CYBERWISER ESSENTIAL	CYBERWISER PLUS
FEATURED				
Registration required	✗	✓	✓	✓
Self Assessment Questionnaire	✓	✓	✓	✓
Vulnerability Testing	✗	✓	✓	✓
Sensors Installation	✗	✗	✓	✓
Real time monitoring	✗	✗	✓	✓
Real time risk assessment	✗	✓	✓	✓
Dashboard	✗	✗	✓	✓
DSS societal impact evaluation	✗	✗	✓	✓
DSS cost-benefit analysis	✗	✗	✗	✓
Risk Modelling system	✗	✗	✓	✓
Risk analytics	✗	✗	✓	✓
WISER online service support	✗	✗	✓	✓
WISER onsite service support	✗	✗	✗	✓
	Get started	Get started	Get started	Get started

IV WISER Cartography: EU National strategies

