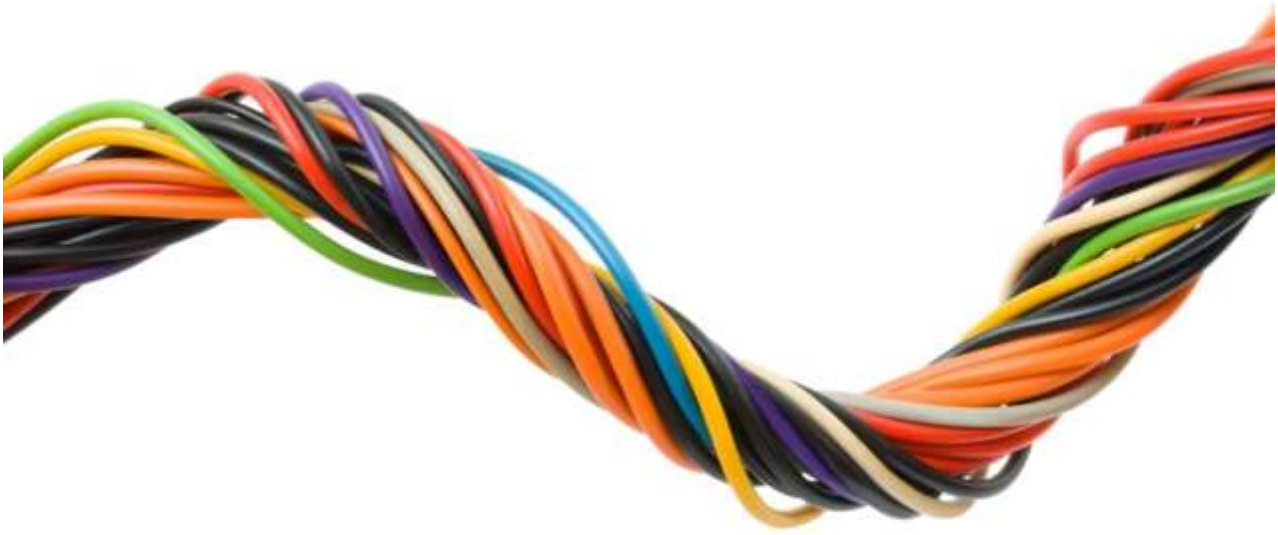
Intended for
ENISA

Document type
Case Study report

Date
May 2016

EVALUATION OF ENISA'S ACTIVITIES

CASE STUDY REPORT – WORK PACKAGE 1.2 2015



RAMBØLL

EVALUATION OF ENISA'S ACTIVITIES
CASE STUDY REPORT – WORK PACKAGE 1.2 2015

Revision	**1**
Date	**27/05/2016**
Made by	**Franziska Lessmann**
Checked by	**Helene Urth**
Approved by	**Helene Urth**
Description	**Case study report – Work Package 1.2 2015**

Ramboll
Square de Meeûs 35,
1000 Brussels
Belgium
T +32 (0)2 737 96 80
F +32 (0)2 737 96 99
www.ramboll.com

CONTENTS

TABLE OF FIGURES

APPENDICES

Appendix 1
Interview Guide
ENISA CASE STUDY interview guide

1. INTRODUCTION

The present report is part of the external evaluation of ENISA's activities in 2015. It takes an in-depth look at one of ENISA's work packages, namely **Work Package 1.2 Improving the Protection of Critical Information Infrastructures**. It is one of four work packages which intended to contribute to ENISA's Strategic Objective 1: To develop and maintain a high level of expertise on EU actors taking into account evolutions in Network and Information Security (NIS). This case study report presents a detailed analysis of the extent to which WPK 1.2 has achieved these objectives and feeds into the answering the evaluation questions as summarised in the evaluation matrix.

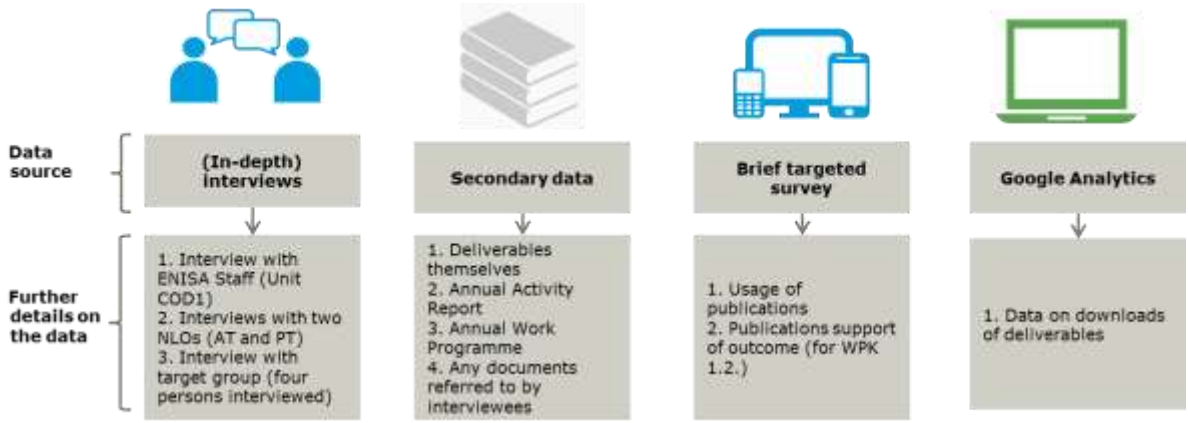
In total, three case studies were conducted to evaluate ENISA's 2015 activities. They each focus on one of the work packages under Strategic Objectives 1 to 3 (SOs). In our selection of work packages (WPK) we have prioritised those with the highest allocation of funds for SO1 and SO2, and for SO3 we have selected the WPK with the second-highest allocation of funds, but which covers other types of tasks which the Agency undertakes. Thereby, we ensure a diverse coverage of ENISA´s tasks as set out in the basic Regulation, Article 3. Within the three selected WPKs, we include all deliverables above €30,000 (in accordance with the framework for the evaluation).

The case study on WPK 1.2 covers four deliverables (with a budget above €30,000):

- D1 - Stock Taking, Analysis and Recommendations on the protection of Critical Information Infrastructures (CIIs)
- D2 - Methodology for the identification of Critical Communication Networks, Links, and Components
- D4 - Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector
- D5 - Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services

The case study report is based on four sources of data in order to ensure as detailed an examination as possible. The figure below summarises these four sources.

Figure 1: Overview of data sources



With regard to the in-depth interviews, a total of ten persons were interviewed including ENISA staff (COD1), two NLOs, and persons from the target group (participants to an e-Health workshop and contributors to publications under this WPK).

The mini-survey was annexed to the general survey on ENISA's 2015 activities. In total, 84 responses were collected and used in the analysis of WPK 1.2. A full overview of the responses to the survey (including the brief targeted survey) can be found in Appendix 5 of the evaluation report. The secondary data (including publications from ENISA), the information on media feedback and the Google Analytics data have been provided to the evaluator by ENISA.

In addition to the survey and the interviews, we have been provided with examples of media feedback on ENISA's deliverables under WPK 1.2. The evidence is also presented in this report.

This case study report is organised as follows:

- Section 2 presents the work package and its deliverables, linking them to the outputs, outcomes and results identified in the intervention logic.
- Section 3 presents the findings for each of the four deliverables with regards to the intended outputs and outcomes based on interviews, survey and the media feedback. Based on these findings, an assessment of results is made.
- Section 4 provides conclusions on output, outcome and result level.

2. BACKGROUND

This chapter presents the overall aim and the specific deliverables under Work Package 1.2 and their intended outputs, outcomes and results as identified in the intervention logic.

WKP 1.2 is part of ENISA's strategic objective (SO) 1: *To develop and maintain a high level of expertise of EU actors taking into account evolutions in NIS*. In its work programme, ENISA notes that ensuring adequate levels of protection for modern IT systems in any context requires recognising and adapting to changes in the evolving threat environment. While not all potential threats can be foreseen, the evolution of some threats can be predicted with accuracy based on past data. Therefore, ENISA can support stakeholders in compiling and analysing relevant data on incidents. Furthermore, ENISA assists the Commission and Member States in training professionals in NIS to meet the requirements of industry at all levels.

In this context, WPK1.2 Improving the Protection of CIIs aims at providing advice and assistance on request to targeted stakeholders of CIIs. The stakeholders can be both public such as the Commission or Member States, and private, like banks, SMEs or eHealth providers.

2.1 Deliverables of the work package

2.1.1 Deliverable 1: Stock taking, analysis and recommendations on the protection of CIIs

As deliverable D1, ENISA published the report "Stocktaking, Analysis and Recommendations on the Protection of CIIs" in January 2016. The report is primarily intended for Member States and the Commission. In addition, the report "CIIP Governance in the European Union Member States" was developed to which according to ENISA's budget implementation access was restricted.[1]

The deliverable is intended to contribute to the improvement of protection of Critical Information Infrastructure in the form of ICT systems considered to be critical infrastructure themselves or ICT systems which are essential for the operation of critical infrastructures (such as telecommunications, computers and software, internet or satellites). It takes stock of and analyses existing measures to enhance CII protection and suggests good practices and recommendations to national authorities and legislators. The aim is to increase resilience and decrease the risk of disruption or failure of critical infrastructure.
The study identifies action areas which contribute to an effective national protection of CII. It presents information collected through interviews and surveys on Member States' relevant governance structures. Finally, general recommendations to Member States and the Commission suggest means to improve CII protection in the EU.

2.1.2 Deliverable 2: Methodology for the identification of Critical Communication Networks, Links and Components

In the development of methodologies for identification of critical communication networks, links and components, ENISA developed a methodology to identify dependencies on communication networks of critical infrastructures as smart grids.
The report "Communication network interdependencies in smart grids" was published in January 2016. It mainly addresses smart grid operators, manufactures and vendors, as well as smart grid tools providers.

The report understands interdependencies in communications between different parts of communication networks as a fundamental pillar of smart grids but also as a point which is sensitive to attacks due to important detail of transmitted data. Therefore, the study focuses on the evaluation of these interdependencies, including their architectures and connections. Through interviews with experts in the field their importance, threats, risks and mitigation factors are identified.

Two main types of concerns were expressed by the experts: technical and organisational ones. Based on the findings, seven recommendations to the European Commission, Member States and

[1] The analysis was focused on the main report.

operators of smart grids, as well as manufacturers, vendors and asset owners are presented on how to reduce risks for smart grids.

2.1.3 Deliverable 4: Recommendations and good practices for the use of Cloud Computing in the area of Finance Sector

Published in December 2015, the report "Secure Use of Cloud Computing in the Finance Sector. Good practices and recommendations" is primarily intended for banks and industry stakeholders.

The report assesses the usage of private and public Cloud options in the European financial industry. It identifies challenges to be addressed by cloud market players and highlights the most pressing short-term issues linked to the promotion of cloud services. In addition, long-term challenges are discussed. Based on the analysis the report provides recommendations to financial institutions, regulators and cloud service providers about what should be done to support secure adoption of cloud services in the finance sector.

2.1.4 Deliverable 5: Good practices and recommendations on resilience and security of eHealth Infrastructures and Services

The report "Security and Resilience in eHealth. Security Challenges and Risks" was published in December 2015 under the work of deliverable 5. It was accompanied by an annex with country reports on security and resilience in eHealth with restricted access. Target readers of the report are eHealth providers, the Commission and the Member States.

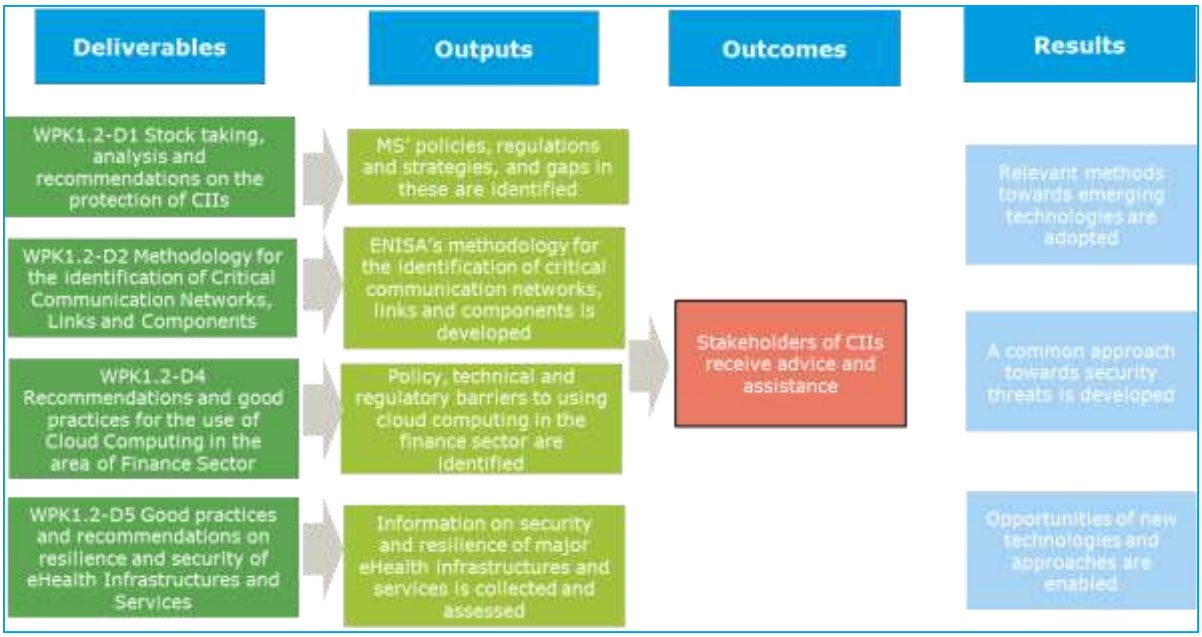
The study identified the different approaches and measures taken by Member States to protect critical healthcare systems which aim at improved healthcare and patient safety. In this respect, the study analysed the political and legal context in Member States, the perception of critical assets in eHealth infrastructures, as well as security challenges and requirements. Good practices were identified. In a survey different uses of eHealth which were considered most critical were identified, namely Cloud Services supporting eHealth, Electronic Health Records /Patient Health Records and national eHealth services (i.e. ePrescription). For these fields nine recommendations addressing Member States and operators of eHealth infrastructures were provided.

2.2 Intervention logic

The figure below presents an extract of the intervention logic for Strategic Objective 1. It focusses on the deliverables under Work Package 1.2.

An intervention logic is a systematic and reasoned description of the casual links between the Agency's activities, outputs, outcomes, results and impacts. It helps to understand the objectives of the Agency as a whole and its specific deliverables.

Figure 2: Intervention logic for Work Package 1.2 (deliverables over EUR 30,000)



The findings presented below have been structured according to the outputs, outcomes and results listed above in relation to the deliverables of Work Package 1.2. Making a judgement in relation to the degree of achievement of the intended outputs and outcomes of the deliverables enables conclusions to be drawn on the extent to which ENISA is having an impact on NIS.

3. FINDINGS

3.1 Deliverable D1 Stock Taking, Analysis and Recommendations on the protection of CIIs

In order to follow up on achievements of the different deliverables, ENISA sets Key Impact Indicators (KIIs) which are presented in the annual work programmes. The annual activity report reports on the extent to which the KIIs have been achieved.[2] By the end of 2015, ENISA partially achieved the aims set for D1, as presented in Table 1. More than 16 Member States have been involved in ENISA's work around Critical Information Infrastructure Protection (CIIP). It can however not be said yet whether they will take ENISA's findings and good practices into account in their own strategy. The targeted number of stakeholders has been reached in the work on developing a methodology on internet connections. Member States have shown interest in ENISA's work on government cloud good practices. By 2016, ENISA aims to have five Member States use the good practices for their national strategy.

Table 1: Impact indicators and achievements for D1

Impact indicators	Achievements by the end of 2015
By 2017, 8 Member States (MS) use ENISA's findings and good practices in their national CIIP strategies	• One workshop in September about CIIP. More than 8 MS participated in the workshop, more than 16 MS took part in interviews and surveys providing input for the study.
Engaging 8 public and 8 private stakeholders (ISP, IXPs, Telcos) in the development of the methodology on internet interconnections	• One workshop in October about communication network dependencies for smart grids study (25 experts from national authorities and critical infrastructure operators in Europe) • One meeting in November of the Internet Infrastructure Security and Resilience Reference group of experts (INFRASEC 14 experts: 2 cyber sec agencies, 3 major IXPs in Europe, 2 Internet security research organization) • Study completed and dedicated resilience portal area about Internet threats created.
By 2016, 5 MS use ENISA's government cloud good practices on in their national strategy	• One workshop in June on Cloud Security (50 participants, more than 25 from private sector). In this event a session on Governmental Clouds was created with the participation of experts from 3 Member States: Estonia, UK, Netherlands

3.1.1 Output: Identification of Member States' policies, regulations and strategies, and their gaps

Downloads

The report "Stocktaking, Analysis and Recommendations on the Protection of CIIs" was downloaded 886 times between its publication in January 2016 and April 15th[3] 2016, of which 49% (438 downloads) were in the EU. Another 21% of downloads were done in Russia while the USA accounted for 12% of downloads and the remaining ones are spread across the globe. While this data does not provide a clear indication whether the output has been reached it shows that there has been moderate interest in the publication. Downloads are far from being as high as for D4 and D5 (as presented below).

With regards to the downloads in EU, the medium[4] used cannot be determined[5] in 51% of the cases, while 26% of the downloads happen as a result of an organic search[6]. Finally, 22% of the

[2] In the work programme and the annual activity report KIIs are linked to the WPKs but not to individual deliverables. The KIIs have been linked to the different deliverables based on documentation received from ENISA.

[3] The URL changed for the ENISA website on April 15th 2016 and therefore this date is used as a cut-off point. The evaluation which will be carried out by Ramboll next year will examine the number of downloads for the publication for the whole duration of 2016.

[4] Medium refers to how users get to the page where they download the publications.

[5] In a high number of cases Google Analytics cannot determine the referrer who brought the users to the page where he/she downloaded an ENISA publication. Thus, this medium, called "none" in the dataset, does not provide explanatory power in determining how users found the publication, since it can cover a variety of instances, including the two most common which are clicking a link from an email or clicking a link from a Microsoft Office or PDF document.

[6] Organic traffic is all the traffic that comes from unpaid sources on search engines like Google, Yahoo and Bing.

downloads occur as a result of referral[7]. The share of downloads through the different media are mostly comparable with the averages of downloads of deliverables of 2014.

The report was shared over social media, such as Twitter (representing 10% of EU downloads) and LinkedIn (representing 2% of worldwide downloads). With 1.4% of downloads worldwide, the portal FierceGovernment IT on technological developments in the U.S. government also represents an important access point for referral downloads.

The annex "CIIP Governance in the European Union Member States" was downloaded between its publication and April 15th, 2016 no more than 175 times worldwide. The majority of these downloads were outside the EU, with the USA representing 35% and Russia 34%. EU downloads only accounted for 18% (31 downloads).

For 71% of these downloads the medium cannot be determined, 29% of downloads took place as a result of an organic search via google. None of the EU downloads took place after referral.

Online media feedback on the deliverable

The high share of downloads via Twitter of the study "Stocktaking, Analysis and Recommendations on the Protection of CIIs" can be explained by the fact that the report has been referred to in a tweet from Politico's feed on technology policy. The conclusions of the study have furthermore been referred to through a German online information portal on data security (datensicherheit.de). KPMG who contributed the report shared the results on their website. In addition, the British Library has included the report into their catalogue.

Interviews

The interviewees explained that the report was developed in the context of the preparation for the NIS Directive. The deliverable was intended to provide an idea of the gaps in CIIP and how to approach these. Interviewed ENISA staff noted that they were satisfied with the participation of Member States and an EFTA country, and that in turn these provided positive feedback on ENISA's recommendations. Furthermore, they had experienced strong interest from different stakeholders.

Three interviewees were able to comment on the output of the deliverable. They underlined that the reports were very relevant and provided a useful comparison between different Member States. One of them also noted that the recommendations were very useful.

3.1.2 Outcome: Advice and assistance to Stakeholders of CIIs

Survey

According to the survey, 27 respondents had made use of the publication "Stocktaking, Analysis and Recommendations on the Protection of CIIs" and of these 23 agree or strongly agree that ENISA's work, outputs and publications provide stakeholders of CIIs with advice and assistance. The remaining four respondents either did not know, or indicated to neither agree nor disagree. The same number of survey respondents had read the Annex to the report and they shared the same opinion on ENISA's work, outputs and publications.

Interviews

The findings from the interviews suggest that ENISA has managed to achieve the outcome of providing assistance and advice to stakeholders with this deliverable. Three interviewees noted that the deliverable helped Member States to identify their weaknesses by comparing what other Member States would do. The deliverable is used as a starting point to identify differences, understand which questions to ask and where to find support. The report contributes to improved cyber security based on best practices provided by ENISA.

An NLO suggested however, that ENISA's advice and assistance was not equally responding to the needs of all Member States. A Member State which was less in the centre of ENISA's

[7] "Referral" means that the recipient has arrived to the publication by clicking on a link on another website/email.

attention would not be able to make use of ENISA's work to the same extent as other Member States could.

In the context of this deliverable, one interviewee praised ENISA as a neutral agency to give recommendations which could be easily referred to by national policy makers.

Two interviewees highlighted ENISA's capability to bring together the right stakeholders and to set relevant agendas. Both private and public stakeholders could be reached with advice on CIIs. This was also highlighted by ENISA staff themselves. They noted that in the context of the development of this deliverable, a cooperation group was created which will be continued in the future context of the preparation for the implementation of the NIS Directive.

This step forward on the way to implementing the NIS Directive can be considered as an unintended outcome. Three interviewees considered the future work of ENISA on the implementation of the NIS Directive to be of very high relevance and saw a role for ENISA to support Member States. One of these interviewees was however concerned that ENISA would be missing resources to do so.

3.2 Deliverable D2 Methodology for the identification of Critical Communication Networks, Links, and Components

The KIIs set for D2are equal to the first and third indicator of D1, as shown in Table 2 below. Again, ENISA has been able to make progress towards reaching the number of targeted Member States by 2017 and 2016 respectively.

Table 2: Impact indicators and achievements for D2

Impact indicators	Achievements by the end of 2015
By 2017, 8 MS use ENISA's findings and good practices in their national CIIP strategies	• One workshop in September about CIIP. More than 8 MS participated in the workshop, more than 16 MS took part in interviews and surveys providing input for the study.
By 2016, 5 MS use ENISA's government cloud good practices on in their national strategy	• One workshop in June on Cloud Security (50 participants, more than 25 from private sector). In this event a session on Governmental Clouds was created with the participation of experts from 3 Member States: Estonia, UK, Netherlands

3.2.1 Output: Methodology for the identification of critical communication networks, links and components

Downloads

In total, this deliverable was downloaded 737 times worldwide between its publication in January 2016 and April 15th 2016, of which 42% (306) occurred in the EU. Furthermore, the report was downloaded 91 times in the USA (12% of downloads) and 76 times in Russia (10% of downloads). The share of downloads was surprisingly high in Iran (2%) and Ethiopia (3%). The limited target group might explain the rather moderate number of downloads.

In relation to the mediums used to generate EU, this deliverable stands out for the high share of downloads occurring after an organic search: 46% of downloads have been done this way, primarily through google and bing (the average for 2014 deliverable was of 23%). For 45% of the downloads it is not possible to determine the referral, while for only 9% the referral was identified.

Online media feedback on the deliverable

Continuity, Insurance & Risk Magazine on risk management, business continuity and commercial insurance wrote a short article on the report entitled "Smart grid vulnerability highlighted in new ENISA report". Two online portals for companies active in NIS published further short articles on the report (Continuity Central and Help Net Security), and a blog on NIS for governments and companies wrote a post on the report.

In addition, Günther Oettinger, Commissioner for Digital Economy & Society tweeted about the report. The tweet did not provide a direct link to the report which to some extent can explain the high share of downloads after organic search.

Interviews

The relevance of the Commissioner's tweet was also highlighted by the interviewed ENISA staff. They underlined that it was important to raise awareness among stakeholders and to provide guidelines on using smart grids but also explaining potential attack scenarios. Based on positive feedback received, the scenarios will be further developed in 2016. ENISA was very satisfied with the received media feedback on this deliverable.

Further interviewees had only limited knowledge of the deliverable. One NLO underlined that his Member State planned to look further into the field of smart grids in the future and that in this context the deliverable was probably going to be useful.

3.2.2 Outcome: Advice and assistance to Stakeholders of CIIs

Survey

According to the survey, 29 respondents had made use of the publication under D2 and of these 26 agree or strongly agree that ENISA's work, outputs and publications provide stakeholders of CIIs with advice and assistance. The remaining three respondents either did not know, or indicated to neither agree nor disagree.

Interviews

ENISA staff showed satisfaction with the work on the deliverable as 25 experts and national authorities were involved which would be using the deliverable for further work to secure smart grids. The same satisfaction was however not shared by the other interviewees.

While two interviewees underlined that the work of ENISA in the field of CIIs was very important, specifically in order to raise awareness, they were not able to refer to how stakeholders had used ENISA's advice to secure smart grids. The only outcome reported by one interviewee was that ENISA worked as a facilitator between different stakeholders of smart grids and could help here with recommendations and setting requirements. Again ENISA was highlighted as a neutral party to turn to for advice. The same interviewee also suggested, however, that ENISA needed more personnel to grasp the complexity of the different fields surrounding CIIP. In particular the limited amount of time for which experts could be contracted by ENISA was criticised. Where experts would work with ENISA for two or three years, any expertise that was build up over that period, would be lost for ENISA once the contract ended.

3.3 Deliverable D4 Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector

For D4, ENISA measures its achievements in terms of the number of Member States and private stakeholders that use the recommendations on finance in their risk assessment and management approach (see Table 3). There has been strong interest from the national financial regulators and private banks, as well as cloud service providers in ENISA's activities in this field. The indicator has, however, not been reached yet.

Table 3: Impact indicators and achievements for D4

Impact indicators	Achievements by the end of 2015
5 MS and 5 private stakeholders use ENISA's recommendations on finance in their corporate/national risk assessment and management approach	• One workshop in October in cooperation with European Banking Authority (EBA). In this event participated 26 EU national financial regulators, 12 EU private banks and 4 major Cloud service providers • The Expert Group in Finance was engaged and on

	average 15 experts from financial private sector were participating.

3.3.1 Output: Identification of policy, technical and regulatory barriers to using cloud computing in the finance sector

Downloads

D4 reached an impressive number of 4061 downloads worldwide between its publication date and April 15th 2016. Considering that this deliverable was only published in December 2015, the number of downloads is high compared to the average download of deliverables in 2014 (which was 6724 over a period of a minimum of 13 months). This volume of downloads testifies to the popularity and general usefulness of the deliverable, especially considering the limited target audience of the finance sector. In addition, 62% of these downloads (2528) were made in the EU, furthermore suggesting that ENISA reached its target audience with the report. Downloads from the USA accounted for 17% while the rest was spread around the globe. On average, 46% of downloads of deliverables from 2014 were downloaded in the EU.

In most cases (48%) it was not possible to establish the referral of the EU downloads. Compared to the averages for deliverables of 2014, downloads following organic searches were rather low with 18%, while the share of referrals was with 33% rather high. Most importantly, the European Banking Authority noted on their website that they acknowledged the report which can be accounted for 649 downloads (16% of worldwide downloads). Furthermore, social media such as Twitter, Facebook and LinkedIn generated a number of downloads through referral (circa 4% of worldwide downloads).

Online media feedback on the deliverable

In addition, to the acknowledgement of the European Banking Authority, the conclusions and recommendations of the report were published on the website of SLA-Ready, an organisation supporting the private sector with access to cloud service level agreement. A research platform on legal questions (Lexology) and a blog about worldwide financial services regulation (Regulation Tomorrow) published articles on the report presenting its conclusions. Furthermore, the findings of the report were referred to by the information portal of IBM, Security Insight. In its blog, the CFA institute, which educates financial analysts referred to the report.

Interviews

ENISA staff underlined that the report was intended to provide guidance for cases where banks using cloud services operate in more than one Member State. Three types of stakeholders were targeted with the deliverable: cloud service providers, financial regulators and financial institutions. Unfortunately, it has not been possible to interview these stakeholders for the case study.

ENISA staff noted that they had been working very closely with the different groups and aimed at meeting their needs. It was specifically mentioned that cloud service providers agreed to all recommendations provided in the context of the deliverable.

Two of the other interviewees highlighted cloud technology and the finance sector as very important topics which should certainly be looked into from the perspective of CIIP.

3.3.2 Outcome: Advice and assistance to Stakeholders of CIIs

Survey

The survey results show that 30 respondents had made use of the publication under D4. Out of these, 22 agreed or strongly agreed that ENISA's work, outputs and publications provide stakeholders of CIIs with advice and assistance. Seven respondents neither agreed nor disagreed with the statement, while one user of the publication did not know.

Interviews

ENISA considered their work on this deliverable as very important to provide assistance to stakeholders. In the interview ENISA staff underlined that the work on this deliverable had brought together all relevant stakeholders for a first time to discuss cloud computing in the finance sector. This cooperation led to an important change in perception: it was noted that regulators were not generally against the use of clouds as others had been assuming but understood that regulators had an important position to help could providers to create a sufficiently high level of security.

This finding could not be confirmed by the other interviewees. The two NLOs noted that in their countries the report had been used to gather information for decision making. One of them noted, however, that there are always numerous sources taken into consideration in decision making and that therefore the contribution of the specific deliverable was not certain. Consequently, the contribution to the outcome cannot be assessed.

3.4 Deliverable D5 Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services

The impact indicator for D5 sets a target in terms of Member States and private stakeholders using ENISA's recommendations on e-Health in their risk assessments or management approaches, as shown in Table 4. By the end of 2015, Member States and e-Health providers had shown interest in these activities by participating in workshops and contributing to a study.

Table 4: Impact indicators and achievements for D5

Impact indicators	Achievements by the end of 2015
5 MS and 5 private stakeholders use ENISA's recommendations on eHealth in their corporate/national risk assessment and management approach	• Participation to workshop of 10 MS, 10 eHealth providers and the EC • Twelve MS participated in the study/survey

3.4.1 Output: Collection and assessment of information on security and resilience of major eHealth infrastructures

Downloads

In total, the report "Security and Resilience in eHealth. Security Challenges and Risks" was downloaded 2025 times worldwide between its publication in December 2015 and April 15th 2016, of which 45% (920) occurred in the EU, and the United States accounting for 26% (520) of the downloads. The remaining 27% are accounted for by many other third-counties, including the Ukraine with 241 downloads (12% of all downloads). The total number of downloads suggests a strong reach, considering that on average deliverables of 2014 were downloaded 6724 times in 13 months. In particular, the rather targeted audience of the health sector leads to the conclusion that the report was of significant popularity.

In relation to the mediums used to generate EU downloads, the report is very similar to the average of deliverables from 2014: for 60 % of downloads it is not possible to determine the referrer, 23% of downloads occurred after an organic search and 17% after referral. For this report Twitter (2% of worldwide downloads) and LinkedIn (3% of worldwide downloads) showed to be important access points. Furthermore, a number of downloads were generated directly through ENISA's website.

Between its publication date and April 15th 2016, the annex to the document was downloaded 135 times. Downloads were made from the EU (42%), Russia (33%) and the USA (15%). The remaining 10% of the downloads were made from a number of countries worldwide.

For a majority of the EU (74%) the referrer is not determined. Downloads after organic search represent 19% and 7% were generated after referral.

Online media feedback on the deliverable

The main report was presented in an article by BNA Bloomberg that provides information for professionals in a number of fields, including taxation, legislation and regulation. The Global Security Mag republished ENISA's notification about the report. Two news portals on e-Health presented the report and linked to it (eHealth News and digitalhealth.net). In addition, Tech Talks Central referred in a radio show on the need for interoperability in eHealth and interviewed an ENISA employee for this purpose.

Interviews

For ENISA, this deliverable was the first time of working in the e-Health field. The interviewed staff members noted that the aim of the deliverable had been to identify the most important infrastructures and services and that based on the findings specific measures for the different assets could be developed. One concern was expressed with regards to the difficulty to communicate with all Member States in this field.

Employees of two national health authorities were interviewed for this case study. They both underlined the relevance of the topic and ENISA's work in this field. One of them furthermore noted that the focus on access controls was specifically important as at national level this area was also being assessed. The other one suggested, however, that the report would be more relevant for providers of health care, rather than policy makers.

Three interviewees mentioned in the context of this deliverable that ENISA reports often tended to be too technical to be relevant at policy level. One of them suggested that ENISA should develop more simple documents on good practices that could more easily be handed over to hospitals themselves, instead of only addressing the technical specialists. Often it would be difficult to understand and then implement ENISA's recommendations. Another of these respondents suggested adding non-technical executive summaries to the reports that could also be used by policy makers.

3.4.2 Outcome: Advice and assistance to Stakeholders of CIIs

Survey

According to the survey, 23 respondents had made use of the publication "Security and Resilience in e-Health. Security Challenges and Risks" and all of them agree or strongly agree that ENISA's work, outputs and publications provide stakeholders of CIIs with advice and assistance.

Interviews

ENISA's aim to generate awareness with this deliverable was also considered to be an important step to take by the different interviewees. As two interviewees underlined, users of e-Health technology would not be aware of the risks related to using ICT and generating health data. However, as explained above, the interviewees rather criticised the high technicality of the report while ENISA staff noted the provision of guidelines at a more technical level to be a positive achievement.

With the work on the deliverable, ENISA has again played an important role to bring stakeholders together according to two interviewees. ENISA staff noted that they had published a call for experts which will also be used beyond this deliverable.

One of the interviewees suggested that the work of ENISA on e-Health did contribute to providing advice and assistance to stakeholders of CIIs. The deliverable was considered way to support the work nationally done and ENISA's statements would be a useful support to generate more interest and attention at national level. The work done under the deliverable would furthermore provide indications on how to evaluate national networks on e-Health. For this respondent, the deliverable has brought a lot of change and allowed to increase national capabilities. Hospitals would go back to the Ministry of Health and request further information on the data provided by ENISA.

Another interviewee agreed that awareness about resilience and security of e-Health had been increased but noted that this development could not be attributed to a single report. While it could be seen that health care providers brought these issues forward to municipal, regional and national governments, it could not be said that this was due to ENISA's deliverable.

3.5 Contribution towards expected results of the WPK as a whole

This section assesses whether the evidence collected shows that the different deliverables have contributed towards the results of WPK 1.2 as a whole.

3.5.1 Adoption of relevant methods towards emerging technologies

While the evidence collected in the case study does not show that the deliverables have directly helped to adopt relevant methods towards emerging technologies, the case study presents evidence which suggests that the deliverables under WPK 1.2 have contributed towards the identification of relevant methods by:

- Their work in the fields of e-Health, finance and smart grids. ENISA's publications were described as helping to identify barriers. This can be considered a first step to develop methods to respond to any challenges surrounding these technologies.
- Identifying and involving all relevant stakeholders. ENISA was described to be very open and engaging in cooperation with the public sector and the industry.

3.5.2 A common approach towards security threats

The collected evidence does not suggest that the deliverables under WPK 1.2 have contributed to the development of a common approach towards security threats.
Potentially the work on the NIS Directive will take this direction in the future. One of the NLOs argued that in this context, ENISA increasingly achieves to involve all relevant stakeholders for the preparation of the implementation of the Directive.

Another interviewee suggested that ENISA's information on threats in the different fields surrounding new uses of technology was very relevant. Identifying risks could be a first step to setting a common approach towards security threats.

3.5.3 Enabling opportunities of new technologies and approaches

No evidence has been found that the deliverables of WPK 1.2 directly contributed to enabling opportunities for new technologies and approaches.

Both NLOs underlined the relevance of ENISA's work surrounding new technologies which matched national ambitions. They suggested that ENISA was on the right track to identify fields that are relevant today but also those that will be relevant tomorrow.

4. CONCLUSIONS

At output level, not all deliverables have reached their impact indicators set by ENISA in the annual work programme yet but findings suggest that ENISA is on a good way to reach these. The collected evidence shows that D1 has been used, although the number of downloads (886) is considerably lower than for D4 and D5 Among the assessed deliverables of WPK1.2, the findings suggest that D1 is the one that has best reached its output, namely to identify Member States' CII policies, regulations and strategies, and their gaps. Both NLOs were considered the deliverable to be of high relevance.

The number of downloads for D2 was even lower than for D1 (737) and based on the interviews it has not been possible to establish whether the output has been reached. The few findings suggest that the work in the field is of relevance to the stakeholders but that D2 for now has rather helped raising awareness about security risks related to smart grids than actually developing a methodology for the identification of critical communication networks, links and components.

D4 reached an important number of downloads (4061) but similar to D2 it has not been possible based on the interviews to establish whether the intended output has been met. The interview with ENISA staff suggested that at least a part of the policy, technical and regulatory barriers to using cloud computing in the finance sector have been identified but this could not be confirmed by other interviewees.

Considering the high number of downloads (2025) and the positive feedback from the interviewees, it can be assumed that D5 has at least partially met its output to collect and assess information on security and resilience of major e-Health infrastructures. Interviewees criticised, however, the high technicality of the deliverable which made it difficult to understand for readers with a non-technical background.

At outcome level, the survey provides an indication that the four deliverables have indeed contributed to providing advice and assistance to stakeholders of CIIs. The evidence from the interviews suggests quite strongly that with D1 ENISA has managed to reach the intended outcome. Interviewees agreed that the deliverable contributed to identifying weaknesses in their approach to CIIs and ways to address these. In addition, the deliverable led to an unintended outcome of supporting the preparation of the NIS Directive.

For D2 it is less clear whether the outcome has been reached. The interviewees suspected that ENISA would need more staff to actually advice and assist stakeholders of CIIs in relation to smart grids.

Evidence with regards to the achievement of the intended outcome was equally scarce for D4 and D5. The findings suggest that in 2015, the first steps have been made for ENISA to be able to assist and advise stakeholders on e-Health and cloud computing in finance in the future. ENISA's work has contributed to increased awareness and bringing the relevant stakeholders together.

At result level, evidence is particularly scarce. It has not been possible to identify a direct contribution of any of the deliverables to any of the three intended results. Considering the rather recent publication dates of the different reports (five to six month ago), at this point it time it might be too early to fully assess their results. The findings suggest, however, that on the long term, the deliverables will be able to contribute to the results, as ENISA has only started working in the field of the specific CIIs.

APPENDIX 1
INTERVIEW GUIDE

Interview Guide for case study WPK 1.2.

Interviewee	
Organisation	
Date	
Interviewer	

The interviewer will begin by introducing the evaluation, its objectives and scope. Not all questions needs to be probed, but the deliverables should be explored.
Explain that we are interested in understanding how the interviewee has experienced the WPK, in this case WPK 1.2. Explain briefly what the WPK was intended to achieve.

Remember to adjust your use of the questions if the interviewee answered the survey – check before hand, and ask the interviewee (NLOs may not have been selected through the survey but by ENISA, and may still have answered the survey)

Introductory questions

- What is your main area of work, can you briefly describe your main responsibilities?
- How long have you been working in this area?
- Please describe what activities during 2015 which you have been aware of/participated in *(remember to take this into account when you ask the next questions).*

Link in the intervention logic	Interview questions	Interview notes
1. Through its deliverables, WPK 1.2. provides information about NIS threats in the EU to policy makers and public or private sector organisations 2. Through WPK 1.2. deliverables stakeholders of CIIs receive advice and assistance	**How would you describe the overall achievements of WPK 1.2[8] when it comes to providing policy makers and other (public or private sector organisations) with information about NIS threats in the EU?** Is the picture different or similar if you look at the public and private sector? **How would you assess WPK 1.2 contribution giving stakeholders of CII advice and assistance?** Can you provide an example? **Who benefitted from this?** What was the most/least effective that ENISA did to achieve this?	
3. WPK1.2-D1: Stock taking, analysis and recommendations on the protection of CIIs leads to the identification of MS' policies, regulations and strategies, and gaps in these (*output*).	*Note: Remember to cross-check with survey responses once the result is available, if the respondent´s details are derived from the survey!* **Are you aware of any ENISA activities which support the identification of Member States policies, regulations, strategies or gaps?**	

[8] The WPK terminology will only be used in cases where the interviewee is familiar with it, and in this case Unit COD2. Otherwise, "WPK 1.2" is replaced by the "the Agency" or "ENISA".

Link in the intervention logic	Interview questions	Interview notes
	Have you heard of the any publications which share such information? ("CIIP Governance in the European Union Member States" and a restricted report called "Stocktaking, Analysis and Recommendations on the Protection of CIIs")[9]. Have you used this/these publications? Why/Why not? Did anyone you work with use them? **If yes,** *(he/she read/used the publications)* What was useful about this report? Could something have been improved? **In your opinion, has it led to the identification of MS' policies, regulations and strategies, and gaps in these?** **If no,** could you explain why you have not used it/are not aware of it?	
4. WPK1.2-D1: The identification of MS' policies, regulations and strategies, and gaps in these (*output*) leads to policy makers and public or private sector organisations receiving information about NIS threats in the EU (*outcome*).	[If the interviewee assesses that the identification of MS' policies, regulations and strategies, and gaps has improved] **In your opinion and experience, what were the effects of identifying this?** **In your opinion, did this identification improve the information which stakeholders receive about NIS threats in the EU?** Can you provide an example? Could something have been improved?	
5. **WPK 1.2 –D2:** Methodology for the identification of Critical Communication Networks, Links and Components leads to developing ENISA's methodology for the identification of critical communication networks, links and components *(output)*.	*Note: Remember to cross-check with survey responses once the result is available!* **Are you familiar with any relevant ENISA publications concerning the methodology for the identification of Critical Communication Networks, links and components?** (e.g."Methodology for the identification of Critical Communication Networks, Links, and Components" [10]) **If yes,** could you tell me why and how you have used it/them? What did you learn from this publication?	

[9] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

[10] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/communication-network-interdependencies-in-smart-grids/

Link in the intervention logic	Interview questions	Interview notes
	In your opinion, did it help develop ENISA's methodology for the identification of critical communication networks, links and components? **If no,** could you explain why you have not used it? Can you provide an example? Could something have been improved?	
6. WPK 1.2 – D2: Developing ENISA's methodology for the identification of critical communication networks, links and components (*output*) leads to stakeholders of CIIs receiving advice and assistance *(outcomes)*	[If the interviewee assesses ENISA's methodology for the identification of critical communication networks, links and components has been developed**] In your opinion and experience, what where the effects of this this** (i.e. effects of the development of the methodology)? **In your opinion, did it lead to stakeholders of CIIs receiving advice and assistance?** Can you provide an example? Could something have been improved?	
7. WPK 1.2 –D4: Recommendations and good practices for the use of Cloud Computing in the area of Finance Sector leads to identifying policy, technical and regulatory barriers to using cloud computing in the finance sector (*output*).	Are you aware of any **ENISA recommendations and good practices for Cloud computing in finance?** (e.g. the publication "Secure Use of Cloud Computing in the Finance Sector. Good practices and recommendations"[11]) **If yes,** could you explain what this has achieved? Has it helped identify barriers to using cloud computing (e.g. policy, technical and/or regulatory barriers)? If yes, how? **If no,** do you think that recommendations and good practices for the use of Cloud Computing in the Finance sector is a priority for ENISA? Could you elaborate?	
8. WPK 1.2 –D4: Identifying policy, technical and regulatory barriers to using cloud computing in the finance sector *(output)* leads to stakeholders of CIIs	*NB: Continued from above, so if the respondent has already pointed to improved advice and assistance to stakeholders in relation to barriers to using cloud computing in the finance sector, then skip this question.* [If the interviewee assesses that it has helped identify barriers to using cloud	

[11] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/cloud-in-finance

Link in the intervention logic	Interview questions	Interview notes
receiving advice and assistance (*outcome)*	computing] **In your opinion and experience, what have been/or will be the effects of this** (i.e. of identifying barriers to using cloud computing)? **Have you seen any changes stakeholders´ access to advice and assistance?** Could you provide an example?	
9. WPK 1.2 –D5: Good practices and recommendations on resilience and security of eHealth Infrastructures and Services leads to the collection and assessment of information on security and resilience of major eHealth infrastructures and services *(output)*	**Are you aware of any good practices and/or recommendations on resilience/security of eHeath infrastructures and services**? Have you made use of or heard about the publication entitled "Security and Resilience in eHealth. Security Challenges and Risks"[12] Have you made use of or heard about the annexes of this publication, which contain "Countries' Report" (*please note that there is restricted access to this report).* **If yes,** could you explain what this has achieved? Has it helped collect and assess information about the resilience of major eHealth infrastructures and services in the EU? Could you provide an example? **If no,** do you think that good practices and recommendations on resilience and security of eHealth (infrastructures and services) is a priority for ENISA?	
10. WPK 1.2 –D5: The collection and assessment of information on security and resilience of major eHealth infrastructures and services leads to stakeholders of CIIs receiving advice and assistance *(outcome)*	[If the interviewee assesses that information on the security and resilience of major eHealth infrastructures and services has been collected] **In your opinion and experience, what have been/or will be the effects of this** (i.e. the collection and assessment of this information)? **Have you seen any changes in stakeholders´ access to advice and assistance?** Could you provide an example? Could you elaborate?	

[12] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services

11. Do you have anything you would like to add?

Thank you very much for participating in the interview.