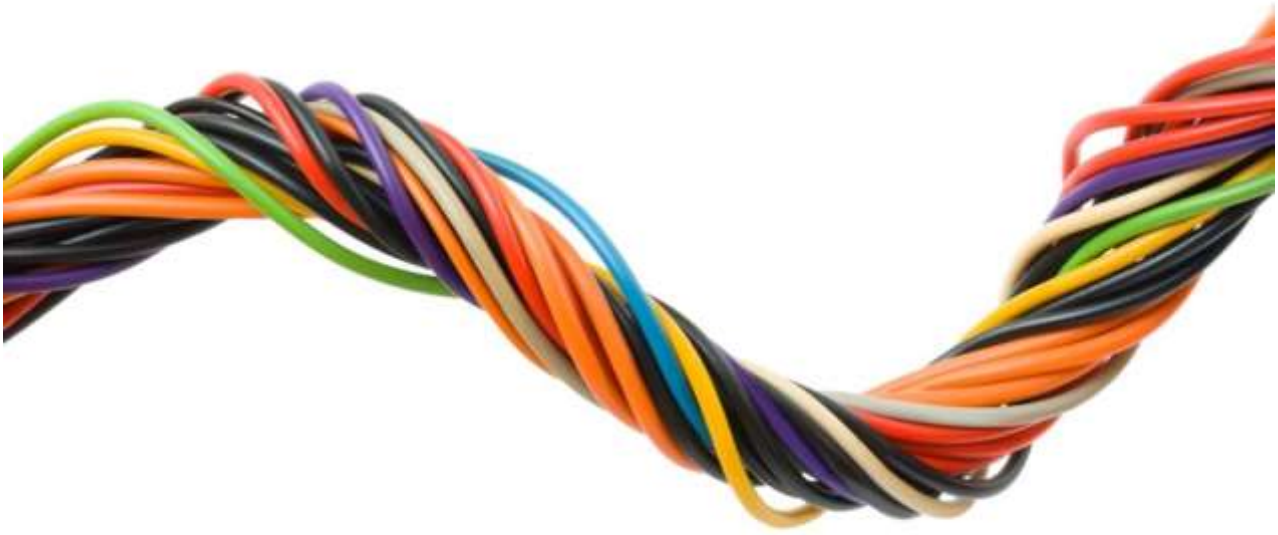
Intended for
ENISA

Document type
Case Study report

Date
May 2016

EVALUATION OF ENISA'S ACTIVITIES

CASE STUDY REPORT – WORK PACKAGE 2.1 2015



RAMBØLL

EVALUATION OF ENISA'S ACTIVITIES
CASE STUDY REPORT – WORK PACKAGE 2.1 2015

Revision	**1**
Date	**27.05.2015**
Made by	**Ida Maegaard Nielsen and Adriana Ilisescu**
Checked by	**Vanessa Ludden**
Approved by	**Helene Urth**
Description	**Case study report – Work Package 2.1 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

1.	**INTRODUCTION**	**1**
2.	**BACKGROUND**	**3**
2.1	Deliverables of the work package	3
2.1.1	Deliverable 1: Support and advise Member States on the establishment and evaluation on National Cyber Security Strategies (NCSS)	3
2.1.2	Deliverable 3: Maintain CERT good practices and training library	4
2.1.3	Deliverable 4: Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap	4
2.1.4	Deliverable 5: Impact evaluations on the usefulness of the ENISA guidelines on capacity building	4
2.2	Intervention logic	5
3.	**FINDINGS**	**6**
3.1	Deliverable D1 Support and advise Member States on the establishment and evaluation on National Cyber Security Strategies	6
3.1.1	Output: Support and advice to Member States on development and implementation of NCSS	6
3.1.2	Outcome: Dissemination of good practices regarding cyber security among public and private organisations	7
3.2	Deliverable D3 Maintain CERT good practices and training library	7
3.2.1	Output: Maintaining and collecting further good practices in different areas of capacity building	7
3.2.2	Outcome: Dissemination of good practices regarding cyber security among public and private organisations	9
3.3	Deliverable D4 Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap	10
3.3.1	Output: Development of a roadmap for updating ENISA's CERT methods	10
3.3.2	Outcome: Dissemination of good practices regarding cyber security among public and private organisations	10
3.3.3	Outcome: Development of Members States' and EU institutions' capabilities in terms of prevention, detection, analysis and response	10
3.4	Deliverable D5 Impact evaluations on the usefulness of the ENISA guidelines on capacity building	11
3.4.1	Output: The assessment of success of past measures and documents supports the development of ENISA Work Programmes in the coming years	11
3.4.2	Outcome: Dissemination of good practices regarding cyber security among public and private organisations	11

3.4.3 Outcome: Development of Members States' and EU institutions' capabilities in terms of prevention, detection, analysis and response 12
3.5 Contribution towards expected results of the WPK as a whole 12
4. CONCLUSIONS 14

TABLE OF FIGURES AND TABLES

Figure 1: Overview of data sources 1
Figure 2: Intervention logic for Work Package 2.1 (deliverables over EUR 30,000) 5

Table 1: Impact indicators and achievements for WPK 2.1 6

APPENDICES

Appendix 1
Interview Guide
ENISA CASE STUDY interview guide

[Short content: Place cursor HERE and insert from menu. Delete the above TOC + pagebreak.]

[DO NOT delete the following line since it contains a section break – delete this field before printing]

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 2.1 Improving the Protection of Critical Information Infrastructures**. It is one of four work packages which intended to contribute to assisting the Member States and the Commission in enhancing capacity building throughout the EU (Strategic Objective 2 (SO2)). This case study report presents a detailed analysis of the extent to which WPK 2.1 has achieved these objectives and feeds into the answering the evaluation questions as summarised in the evaluation matrix.

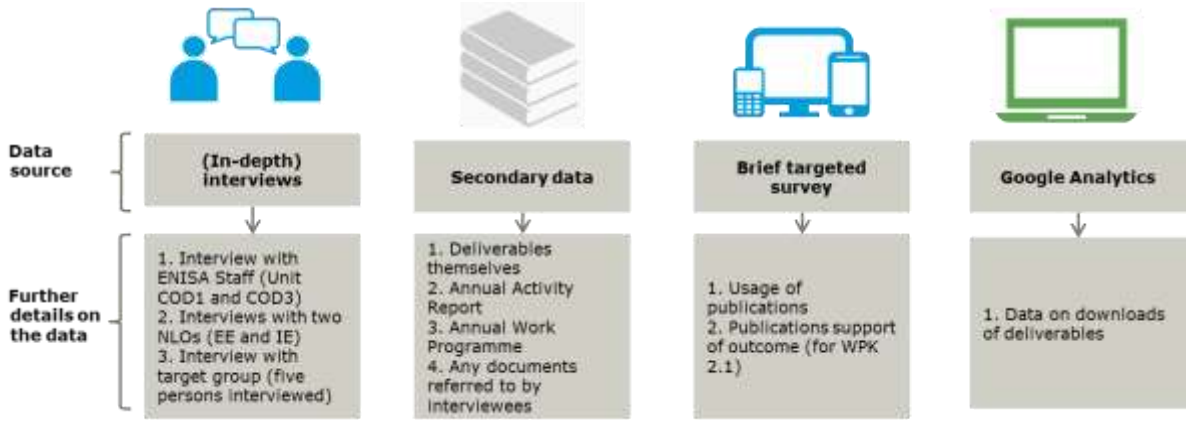
In total, three case studies were conducted to evaluate ENISA's 2015 activities. They each focus on one of the work packages under Strategic Objectives 1 to 3 (SOs). In our selection of work packages (WPK) we have prioritised those with the highest allocation of funds for SO1 and SO2, and for SO3 we 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 2.1 covers four deliverables (with a budget above €30,000):

- D1 - Support and advise Member States on the establishment and evaluation on National Cyber Security Strategies (NCSS)
- D3 - Maintain CERT good practices and training library
- D4 - Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap
- D5 - Impact evaluations on the usefulness of the ENISA guidelines on capacity building

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 and COD3), two NLOs, and five persons from the target group (private sector cyber security experts, and an employee at a ministry of deference).

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 2.1. A full overview of the responses to the survey (including the brief targeted survey) can be found in annex 11 to the evaluation report. The interview guide for the case study is presented in annex 10. 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 were provided with examples of media feedback on ENISA's deliverables under WPK 2.1. 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 at output, outcome and result level.

2. BACKGROUND

This chapter presents the overall aim of WPK 2.1 and its specific deliverables, their intended outputs, outcomes and results as identified in the intervention logic.

The activities developed by ENISA under SO2 are aimed at assisting the Member States and the EU institutions in enhancing capacity building throughout the EU. ENISA's overall goal in connection to SO2 is to work together with Member States and EU institutions to assist them in capacity building across the EU in terms of government, private sector and wider public sector.

In the context of the SO2, the Agency has committed to deliver the WPK 2.1[1] on assisting in public sector capacity building. The WPK 2.1 has the aim of supporting operational bodies and communities (i.e. CERTs and other communities where appropriate) in developing and extending the capabilities necessary to meet the challenges related to network security. A core emphasis in WPK 2.1 is placed on supporting operational bodies and communities by providing advice and support with concrete actions (e.g. CERT training). In addition to this, WPK 2.1 is committed to maintaining and extending the collection of good practice in various areas of capacity building, for example through guidelines for national strategies and exercises and training material for operational communities such as CERTs. The Agency also supports and advises Member States on the development and implementation of National Cyber Security Strategies (NCSS) including identifying the key elements to consider and the most appropriate solutions.

2.1 Deliverables of the work package

In the context of this case study, we focus on deliverables with a budget above EUR 30,000 (the evaluation´s threshold). In each of the following sub-sections, we provide an introduction to the four deliverables which the case study examines.

2.1.1 Deliverable 1: Support and advise Member States on the establishment and evaluation on National Cyber Security Strategies (NCSS)

In 2015, ENISA organised a workshop on *Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA*[2]. The workshop was composed of 3 sessions, i.e.: National Cyber Security Strategies – *An update on the EU situation*, *Critical Information infrastructure protection in the EU*, *Focus on the future of ICS-SCADA in Europe*. The workshop was a one-and-a-half day-long event which gathered the participation of key stakeholders in the field of cyber security[3].

The workshop supported the validation of the results of the ENISA study on WKP 1.2 *Deliverable 1: Stock taking, analysis and recommendations on the protection of CIIs* and of the study WKP 1.2 *Deliverable 3: Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*[4]. The study reveals the current maturity level of ICS-SCADA cyber security in Europe and identified good practices utilised by Member States to improve the area. Additionally, the study informs stakeholders on the current activities developed by Member States in the area of ICS-SCADA.

In support of the National Cyber Security Strategies, ENISA also maintained throughout 2015 an interactive NCSS map, with information on the strategies of Member States, as well as other countries around the world. According to the Annual Activity Report, the map is one of the most popular sites of ENISA and ENISA receives information to make sure it is regularly updated.

The deliverable was intended to: (a) provide support and advice to Member States on the development, implementation and evaluation of National Cyber Security Strategies, (b) provide an update on the national cyber security and critical information infrastructures approaches, (c) foster discussions on specific topics included in the national cyber security strategies, (e) validate

[1] In addition to WPK 2.1, the SO has two additional WPs, i.e. WPK 2.2 – Assist in private sector capacity building, WPK 2.3 – Assist in improving awareness of the general public.
[2] https://www.enisa.europa.eu/events/cyber-security-strategies-critical-information-infrastructures-protection-and-ics-scada-workshop
[3] In addition to this workshop, a workshop was held in Riga in 2015, in connection with the Latvian Presidency. While this workshop is not the focus of D1 under the case study, it is referred to under findings, because it was mentioned by two interviewees.
[4] See: https://www.enisa.europa.eu/publications/maturity-levels

the results of the ENISA studies on Critical Information Infrastructure Protection and ICS SCADA, (e) bring together stakeholders from public and private sector.

2.1.2 Deliverable 3: Maintain CERT good practices and training library

ENISA developed a number of handbooks in the area of CSIRT good practices to further strengthen the knowledge-base of the trainers and maintain an up-to-date training library. The handbooks developed by ENISA to support good practice on CERT encompass:

- "Mobile Threats Incident Handling. Handbook, Document for teachers"[5]: The handbook is aimed at supporting teachers in introducing students to new concepts, tools and techniques used for Mobile and Network Forensics. The targeted audience of the training is CSIRT staff involved in the process of incident handling, especially those responsible for detection of new threats related directly to the CERT customers.
- "Introduction to advanced artefact analysis. Handbook, Document for teachers"[6]: The handbook was developed to introduce CSIRT staff and incident handlers involved in the technical analysis of incidents to advanced artefact analysis.
- "Advanced dynamic analysis. Handbook, Document for Teachers"[7]: The handbook was developed for teachers and is aimed at supporting them in instructing trainees on the methods and techniques of dynamic artefact analysis with the use of OllyDbg debugger package. The target audience for the handbook is CSIRT staff involved with the technical analysis of incidents, in particular those dealing with the sample examination and malware analysis.
- "Advanced static analysis. Handbook, Document for teachers"[8]: The handbook was developed to support training on all aspects of statistic artefact analysis. The target audience is CSIRT staff involved with the technical analysis of incidents, in particular those dealing with the sample examination and malware analysis.

This deliverable was intended to support the dissemination of good practices among target audiences and to build a training library.

2.1.3 Deliverable 4: Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap

The Agency has developed a *Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations*[9] which takes stock of the current situation on vulnerability disclosure, assesses the key challenges in relation to vulnerabilities in computer-based systems, identifies good practices for the various stakeholders involved and provides a series of recommendations for improving the status quo in the vulnerability disclosure landscape.

This deliverable was intended to expand upon previous evaluation efforts in view of building capacity in CERT and proposing a roadmap.

2.1.4 Deliverable 5: Impact evaluations on the usefulness of the ENISA guidelines on capacity building

ENISA published a report titled *ENISA's CSIRT-related capacity building activities*[10] in November 2015. The report presents an updated impact assessment of ENISA's support to CSIRTs in 2014 and served as a basis for the proposed roadmap to 2020. The report assessed the impact of ENISA's support to CSIRT community from a dual perspective – legislative and regulatory, as well as operational. The key objectives of the impact assessment were to support the update of policy analysis, gather additional input from practitioners, including specific input on any new duties and propose concrete actions towards the roadmap implementation.

The deliverable was intended to evaluate the usefulness of ENISA guidelines on capacity building, in view of setting the grounds for the roadmap to 2020.

---

[5] https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/mobile-threats-incident-handling-part-ii-handbook-document-for-teachers

[6] https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/introduction-to-advanced-artefact-analysis.pdf

[7] https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/dynamic-analysis-of-artefacts-handbook.pdf

[8] https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/static-analysis-of-artefacts-handbook.pdf

[9] https://www.enisa.europa.eu/activities/cert/support/vulnerability-disclosure/

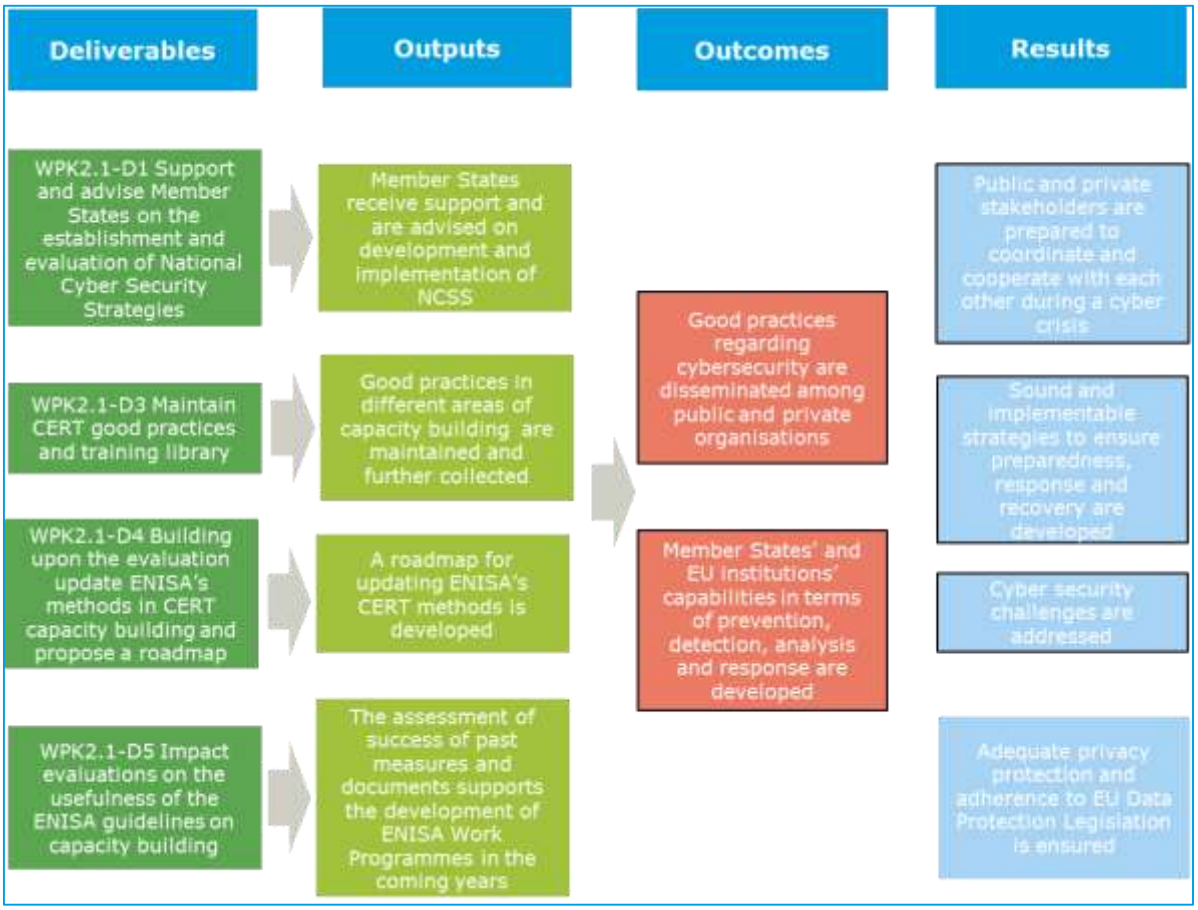
[10] https://www.enisa.europa.eu/publications/leading-the-way-enisa-s-impact-in-operational-security

2.2 Intervention logic

The figure below presents an extract of the intervention logic for Strategic Objective 2. It focusses on the four deliverables under Work Package 2.1 which are above the evaluation´s aforementioned threshold.

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 link this to its specific deliverables.

Figure 2: Intervention logic for Work Package 2.1 (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 2.1. Making a judgement in relation to the degree of achievement of the intended outputs and outcomes of the deliverables will enable conclusions to be drawn on the extent to which ENISA is having an impact on NIS.

3. FINDINGS

In this chapter, we present the findings on the extent to which D1, D3, D4 and D5 under WPK 2.1 have reached the intended outputs, outcomes and, in combination, results as set out in the intervention logic described above.

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. [11] By the end of 2015, ENISA is on a good track to reach the aims set for WPK 2.1, as presented in the table below[12].

Table 1: Impact indicators and achievements for WPK 2.1[13]

Impact indicators	Achievements by the end of 2015
By 2017, 8 MS use ENISA's recommendations and good practices on National Cyber Security Strategies.	2015: Two workshops in 2015 together with the EU Presidency (Riga: 30 participants, 15 form MS; Luxembourg: 28 participants, 18 from MS), 4 MS created their national cyber security strategy based on ENISA recommendations (till November 2015), ENISA NCSS map the most popular webpage (features update). In 2016 ENISA will continue work on this topic through updating the NCSS online map, creating training material in a training platform and updating the good practice guide.
By 2017, continued CSIRT training will be provided to a minimum of 20 participants of different organisations in 5 MS.	2015: 11 CSIRT trainings provided in 7 MS for more than 200 participants representing various private and public organisations.
By 2017, Improved operational practices of CSIRTs in at least 15 MS (on-going support with best practices development)	2015: The "Good practice guide on Vulnerability disclosure" was added to the ENISA's online library for CSIRT services and operational practice improvement. The annual CSIRT workshop for national and governmental CSIRTs held in May in Latvia to discuss and address 'the CSIRT role and services during the EU Presidency' topic (40 participants from 17 MS).
More streamlined CSIRT exercise and training material with CSIRT and other operational communities' services and methodologies.	2015: ENISA's start-up train the trainer program. 1st workshop for CSIRT trainers in Europe held in September to streamline CSIRT training material and training methodology development (24 educators from 18 MS including GEANT/TRANSITS; FIRST).

Please note that these KIIs are due by 2017.

3.1 Deliverable D1 Support and advise Member States on the establishment and evaluation on National Cyber Security Strategies

This section presents the case study´s findings on D1.

3.1.1 Output: Support and advice to Member States on development and implementation of NCSS

The focus of this deliverable was to help provide support and advice to Member States on the development and implementation of NCSS. According to the Annual Work Programme, COD1 was responsible for this deliverable, and organised the workshop.

Under D1, two workshops were held in Riga and Luxembourg respectively. As mentioned above, this case study places primary emphasis on the Luxembourg workshop which was organised and sponsored solely by ENISA. Its title was "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA event" and was held in Luxembourg in September 2015.

Based on the evidence derived from the interviews, the workshop had 28 participants from 18 different Member States, showing a good representation across the EU. This participation rate

[11] 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.

[12] ENISA Annual Activity Report 2015

[13] Please note that these KIIs are assessed in detail in the evaluation report, and that for WPK 2.1, the achievement is deemed partial.

was underline as very positive. While the KIIs report that by November 2015 four Member States had created NCSS based on ENISA recommendations, an interview suggested that by April 2016, six Member States had used the recommendations to devise their NCSS (DK, HR, IE, LU, MT, SK).

Interviewees highlighted that the workshop provided support and advice to Member States by including industry stakeholders (e.g. from finance and manufacturing) to get perspectives on the implementation of NCSS (which needs to be done by both public and private sector).

In relation to the Riga workshop, one interviewee highlighted that this workshop looked more into how NCSS could be implemented and continuously reviewed. One of the big take away points of this workshop was that NCSS needed to be working documents for Member States, so that they are adjusted to take into account new challenges and opportunities.

Three interviewees did not participate in the workshop.

3.1.2 Outcome: Dissemination of good practices regarding cyber security among public and private organisations

In the survey, 23 respondents noted that they were familiar with the workshop, "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA event" and 21 respondents agree that the workshop has helped disseminate good practices regarding cyber security among public and private organisations. This provides some confirmation of the output for D1 (and for this workshop in particular).

Since only few of the interviewees participated in one of the workshops (Riga), they found it difficult to assess the effects of the workshop. However, all two noted that they have heard good feedback on both workshops, referring to the exchange of good practices regarding cyber security, which is the intended outcome of this deliverable (further information in section 3.1.2 below). This is corroborated by the achievement on the KII, stating that ENISA supported Member States in developing their NCSS on the basis of ENISA´s recommendations. Three interviewees underlined that ENISA has too low visibility when it comes to these events, and that more could be done to showcase ENISA´s "high level of expertise" to further boost its impacts.

3.2 Deliverable D3 Maintain CERT good practices and training library

This section presents the case study´s findings on D3.

3.2.1 Output: Maintaining and collecting further good practices in different areas of capacity building

D3 – Introduction to advanced artefact analysis

While the data does not provide a clear indication that the output has been reached, it does suggest that there has been a moderate interest in the publication. In total, this deliverable was downloaded 619 times worldwide between its publication date on 1st of December 2015 and 15th of April 2016, of which 56% (i.e. 349 downloads) were in EU Member States. It should be noted that amongst EU Member States, the downloads were accounted for to a substantive proportion by Croatia (30% of the total number of downloads in the EU, i.e. 194 downloads). As regards downloads from outside the EU, the highest proportion of downloads were by a number of third-countries, primarily Russia (33% of downloads in third-countries) and the United States (15% of downloads in third-countries).

Concerning the downloads in the EU, the medium[14] utilised could not be determined[15] in 74% of the cases (i.e. 259 downloads), while in 17% of the cases the downloading happened as a result

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

[15] 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.

of an organic search[16]. Moreover, the data indicates that this occurred as a result of referral in only in 9% of the cases in which the publication was downloaded in the EU.[17] This is a comparatively low number, given that the average percentage of downloads through referral across all publications from 2014 (as part of the AWP) was 16%. This indicates a moderate level of dissemination of the publication through active referrals, in contrast to cases where users find the publication on their own.

D3 – Advanced dynamic analysis

Overall, the number of downloads suggest some interest in the handbook within the EU, while the United States accounts for the highest number of downloads. In total, this deliverable was downloaded 1,466 times on a worldwide scale between the date of its publication, 1st of December 2015, and 15th of April 2016. Out of the total number of downloads, 68% (i.e. 1,000) were in third countries, whereas 32% (i.e. 462) were in EU Member States. On a global scale, the highest proportion of downloads of the publication in third countries was by users in the United States (60%, i.e. 599 of the total number of downloads in third countries), followed by Russia (11%, i.e. 113 downloads of the total number). In the EU Member States, the deliverable was most downloaded in Croatia (27%, i.e. 129 downloads of the total number of downloads made in the EU Member States), followed by France (21%, i.e. 100 downloads).

The figures provide a clear indication that the level of dissemination through referral of the publication was very low overall. In the case of both the EU and third countries, the medium of download utilised could not be determined in a very high proportion of cases, namely 80% of the cases in the EU and 90% of the cases in third countries. In the EU, downloads were made in an organic manner to a larger extent than through referral. The number of cases in which the download happened as a result of organic traffic was 63 (i.e. 14% of cases of downloads in the EU), whereas the number of cases in which the download occurred as a result of referral was comparatively lower (i.e. 27, i.e. 6% of the total number of cases of downloads in the EU). In the case of downloads from third countries, the situation is similar. The proportion of downloads due to organic search was considerably higher (4%) than that of downloads through referral (1.4%).

D3 – Advanced statistical analysis

The data on downloads clearly indicates a much broader reach of the publication outside the EU than within the EU Member States. In total, this deliverable was downloaded 859 times between 1st of December 2015 and 15th of April 2016, with the highest proportion of downloads being in third countries (70%, i.e. 604 downloads) and with only 30% of total downloads (i.e. 255 downloads) in EU Member States. Similar to the previous handbooks, the highest proportion of downloads within the EU was in Croatia (i.e. 70 downloads, 27% of the total number of downloads from the EU), followed by Greece (i.e. 28 downloads, 11%). Amongst third countries, the highest share of downloads was from the United States (i.e. 49% of downloads in third countries), Iran and Russia (approximately 15% of downloads in third countries for each).

In terms of the medium used to locate the publication for download in the case of EU Member States, the medium was not captured in a very high proportion of cases (77% of downloads in the EU). The web-analytics data indicates that the share of cases in which the downloading of the report happened as a result of organic search was threefold higher (i.e. 24% of cases) than in cases where the download happened as a result of referral (i.e. 8% of cases). The figures suggest a relatively low visibility of the publication as a result of referral.

D3 – Mobile Threats Incident Handling Handbook

In total, this deliverable was downloaded 810 times between the time it was published, 1st December 2015 and 15th of April 2016. The highest share of downloads was from users in EU Member States (59%, i.e. 477 downloads), in contrast to the number of downloads in third countries (i.e. 40%, i.e. 328 downloads). In the EU, the highest proportion of downloads was accounted for by Poland (134 downloads), followed by United Kingdom (105 downloads). In the case of third countries, the highest number of downloads of this deliverable occurred in Russia (79 downloads) and United States (62 downloads).

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

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

Within the EU, the medium utilised to download the deliverable could not be identified in a very high proportion of cases (i.e. 77% of cases). The proportion of cases in which the download occurred through organic traffic and the proportion of cases in which the download occurred as a result of referral was equal (11%).

Overall

The evidence available suggests that ENISA has collected and maintained capacity building in a variety of areas, thus reaching the intended output. Interviewees noted that the dissemination of the handbooks could have been better, and further details are provided on this in the following section.

3.2.2 Outcome: Dissemination of good practices regarding cyber security among public and private organisations

According to the survey, on average, only approximately 17 respondents out of the 82 respondents had made use of the publications on "Advanced Dynamic Analysis. Handbook, Document for Teachers", "Advanced statistical analysis" and "Mobile Threats Incident Handling Handbook"[18] and only 6 respondents indicated that they made use of all three of them. However, out of all the respondents that made use of all three publications, all of them agree or strongly agree that ENISA has led to the dissemination of good practices regarding cyber security among public and private organisations.

Amongst the three outputs under deliverable D3 - Maintain CERT good practices and training library, the ones that had a slightly lower degree of utilisation amongst stakeholders were the publications on advanced dynamic (13 respondents) and statistical analysis (12 respondents), whereas in the case of the publication on "Mobile Threats Incident Handling Handbook", a number of 26 respondents confirmed that they made use of the publication. When asked to assess whether ENISA's work contributed to the dissemination of good practices on cyber security, almost all respondents (i.e. 9 out of 11) that made use of the publication on advanced dynamic and respectively advanced statistical analysis had a positive assessment of ENISA's contribution. Specifically in the case of the respondents that made use of the publication on "Mobile Threats Incident Handling Handbook", almost all respondents (i.e. 23 respondents) strongly agree or agree with the fact that ENISA contributed to the dissemination of good practices regarding cyber security, whereas a number of 3 respondents were unable to assess ENISA's contribution.

Overall, interviewees confirmed that the handbooks were useful – and two of them underlined that these methodologies were used on a day-to-day basis. Interviewees assessed that the training material was useful for the CSIRT community and that ENISA´s work on training in 2015 has helped disseminate good practices.

At the same time, it was suggested that some stakeholders who would value this material are not benefitting, since they are not aware of its existence. Interviewees noted that this is a pity, when such stakeholders could get access to the material on ENISA´s website. In this regard, one interviewee underlined that the most important actors to disseminate to are usually found in one of the following:

- TF-CSIRT (Europe);
- FIRST (global Forum for Incident Response and Security Teams), and;
- The national CSIRT teams.

In relation to this, it was noted that members of national CERT teams (but also from EU CERTs and organisational CERTs) are taking part in the TRANSIT events[19]. ENISA contributes to these training activities with expertise in different fields and thereby largely supports the development of NCSS. In addition, it should be taken into account that other activities take place around the

[18] Note that a question on the extent to respondents have used the publication on "Introduction to artefact analysis" has not been addressed in the framework of the questionnaire.

[19] TRANSIT trainings are conducted under D2 of WPK 2.1, which is not within the scope of this case study. However, it this information is included since it was mentioned by interviewees, and is relevant to confirm ENISA´s familiarity with the CSIRT community.

TF-CSIRT community, bringing various CERT teams together to discuss security matters. ENISA is also present and very engaged in the steering committee of TF-CSIRT, helping to plan activities, and making sure that the programme is relevant and interesting. By playing this role in the governance of such communities, ENISA contributes to the knowledge and expertise of national CERT teams.

3.3 Deliverable D4 Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap

This section presents the case study´s findings on D4.

3.3.1 Output: Development of a roadmap for updating ENISA's CERT methods

D4 – Good Practice Guide on Vulnerability Disclosure, From challenges to recommendations
Overall, the deliverable has been downloaded 2,177 times between the time it was published 18th of January 2016 and 15th of April 2016. This indicates a high degree of interest in the publication when compared with the number of downloads of other deliverables under this WPK. The highest proportion of downloads was made by users from third countries (58%, i.e. 1,268 downloads), whereas users in the EU accounted for 40% of the total number of downloads (i.e. 880 downloads). Amongst European countries, the highest proportion of downloads was accounted for by France (i.e. 18%, 160 of the total number of downloads made in EU countries) and by the Netherlands (i.e. 10%, 92 of the total number of downloads made in EU countries). On the other hand, the highest share of downloads among third countries took place in the United States, which accounted for 869 downloads, i.e. 69% of the total number of downloads in third countries.

In terms of medium, the data shows that in the case of EU Member States, in 60% of the cases, the medium could not be identified, whereas in 17% of cases the report was downloaded as a result of organic search. In contrast, in 23% of cases (i.e. 202 downloads), the download occurred as a result of referral. This is in contrast with the situation for the other deliverables in this WPK where the downloads occurred primarily through an organic search and in a smaller proportion through referral. In addition to this, in 2 cases in the EU Member States (France and Luxembourg), the download occurred through a social medium, suggesting that the publication has been shared through social media.

3.3.2 Outcome: Dissemination of good practices regarding cyber security among public and private organisations

The results of the survey indicate that the publication was utilised to a much higher degree when compared with other publications under this WPK. Respondents were generally aware of and had used the "Good Practice Guide on Vulnerability Disclosure" (38 of the 81 respondents that provided an answer). Out of the total number of respondents that made use of this publication, almost all respondents (31 respondents) agreed or strongly agreed that the work of ENISA has supported the dissemination of good practices regarding cyber security among public and private organisations, whereas the rest were unable to make an assessment.

The survey findings and data on the number of downloads suggest that D4 has been used to a high extent. This finding is also supported by the interviews where two interviewees specifically noted that ENISA published this deliverable at a good point in time, i.e. where there was interest among some Member States to implement better practices on vulnerability disclosure. Two interviewees from private organisations expressed disappointment that they were not aware of this publication, and suggested that ENISA could improve its dissemination of publications, for example through the website LinkedIn. This way, users can also easily share ENISA´s deliverables with their own network.

3.3.3 Outcome: Development of Members States' and EU institutions' capabilities in terms of prevention, detection, analysis and response

According to the result of the survey, out of the total number of respondents that indicated that they made use of ENISA's publication on good practice on vulnerability disclosure (i.e. 38

respondents), half of them (19 respondents) agree or strongly agree that ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States.

According to the data available from interviews, it appears to be too early to judge to what extent the publication has developed Member States capabilities in terms of prevention, detection, analysis and response. All that can be concluded at this point in time is that the publication has raised awareness of the need to implement good practices in vulnerability disclosure. They were unable to provide any specific examples of this. This is exemplified through the following quote:

"It is difficult to say [whether ENISA develops MS and EU capability] – because it is a synergetic approach and it is hard to identify ENISA´s precise contribution. The Agency is one of the few which delivers these trainings and the best practice guides – the only other one is the CSIRT Coordination Centre, but not all of that material is available. Its [contribution] is important".

Due to the sparse data it is difficult to confirm or reject that the publication has contributed to developing Member State´s and EU institutions capabilities in terms of prevention, detection, analysis and response.

3.4 Deliverable D5 Impact evaluations on the usefulness of the ENISA guidelines on capacity building

This section presents the case study´s findings on D5.

3.4.1 Output: The assessment of success of past measures and documents supports the development of ENISA Work Programmes in the coming years

D5 – Leading the way. ENISAs CSIRT-related capacity building activities

In total, the deliverable was downloaded 718 times from the date of publication, i.e. 12th of November 2015, to th 15th of April 2016. The figure indicates a comparatively lower rate of interest or dissemination of the publication both within the EU Member States and in third countries, when considering the other deliverables under this WPK. The number of downloads made by users in the EU amounted to 53% (i.e. 380 downloads), which is slightly lower than the amount of downloads registered in third countries (i.e. 328, 36% of the total). Amongst EU Member States, the amount of downloads in the different states was relatively equal, though a high proportion of the downloads was accounted for by Belgium and France (approximately 15% each of the total number of downloads in EU Member States).

In terms of medium, in the EU, the proportion of cases where the medium could not be identified was half of the total (i.e. 189 downloads). The figures indicate that the dissemination of the report occurred mostly as a result of organic traffic (30% of the cases, i.e. 113 downloads), whereas referral led to only 77 downloads of the report (20% of the total number of downloads in the EU). In 1 case (Ireland), the download occurred as a result of dissemination of the report through Twitter.

According to the results from the survey, the publication was used by a high proportion of respondents (38 of 81 respondents) and that these users were distributed evenly across stakeholder groups. In contrast, 35% of respondents had not made use of the publication at the time of enquiry.

None of the interviewees were able to comment on this deliverable, since they had not heard of it.

3.4.2 Outcome: Dissemination of good practices regarding cyber security among public and private organisations

Out of the total number of respondents to the survey who indicated that they had made use of the publication, almost all respondents (34 respondents) agreed or strongly agreed that ENISA had contributed to the dissemination of good practices regarding cyber security among public and

private organisations, whereas the rest were unable to make an assessment. This is interesting in light of the low number of downloads and no awareness amongst interviewees.

Similar to the case of the other deliverables under WPK 2.1, interviewees noted that in order to improve the dissemination of good practices, awareness of ENISA´s activities and publications should be enhanced. This is reflected in the following quote:

"If I could wish for something, then it would be to create more awareness to keep up to date with people who are engaged with ENISA. It would be nice to hear from them once in a while through a newsletter or something similar".

Due to the limited data available, it is difficult to confirm or reject that the publication has contributed to the dissemination of good practices regarding cyber security among public and private organisations. At the same time, the survey gives some indication that D5 has been useful for stakeholders, but this evidence cannot be corroborated by other sources.

3.4.3 Outcome: Development of Members States' and EU institutions' capabilities in terms of prevention, detection, analysis and response

According to the survey results, 38 respondents made use of the publication and, of these, 30 respondents agree or strongly agree with the fact that ENISA has contributed to the development of Member States' and EU institutions' capabilities in terms of prevention, detection, analysis and response.

The interviewees were unable to assess the contribution of D5 towards the development of Member States capabilities in terms of prevention, detection, analysis and response, since they were not aware of D5 having been published.

Overall, this limited evidence from the interviews means that the case study cannot provide an assessment of the extent to which D5 contributed to the intended outcome, though the survey gives some indication that D5 has been useful for stakeholders.

3.5 Contribution towards expected results of the WPK as a whole

WPK 2.1 was intended to contribute towards four expected results, namely:

1. Public and private stakeholders are prepared to coordinate and cooperate with each other during a cyber-crisis

2. Sound and implementable strategies to ensure preparedness, response and recovery are developed

3. Cyber security challenges are addressed

4. Adequate privacy protection and adherence to EU Data Protection Legislation is ensured

The case study provides some evidence that D1 has given public and private stakeholders opportunities to network and discuss perspectives on the implementation of NCSS, which demands efforts from both sides. However, there is no direct evidence to suggest that any of the deliverables have made a contribution to enabling them to coordinate or cooperate with each other during a cyber-crisis (result no.1).

Regarding WPK 2.1´s contribution to developing sound and implementable strategies to ensure preparedness, response and recovery (result no.2), the case study indicates that D1, D3 and D4 have made contributions to disseminating good practices regarding cyber securities. In particular, D1 is suggested to have made a strong contribution to the development and implementation of NCSS which are intended to improve preparedness, response and recovery.

In relation to whether WPK 2.1 has made a contribution to addressing cyber security challenges (result no. 3), the main finding from the case study is that stakeholders have received increased

access to high-quality information, expertise and an opportunity to learn from other Member States and private stakeholders. While it is not possible to conclude that cyber security challenges have been addressed directly as a result of the deliverables, it is deemed plausible that through D1´s contribution to the development of NCSS (in at least 6 Member States), it has addressed some cyber security challenges.

There was no information available on whether WPK 2.1 has contributed to ensuring that privacy protection and adherence to EU Data Protection Legislation is ensured (result no.4).

4. CONCLUSIONS

At output level, D1 showed the strongest results, and the case study confirmed that ENISA´s workshops in 2015 provided support and advice to Member States on development and implementation of NCSS. In relation to D3, the evidence available suggests that ENISA has collected and maintained capacity building in a variety of areas, thus reaching the intended output. While D4 was shown to have been downloaded to a large extent, and also used by nearly half of the respondents to the survey, it was not possible to confirm or reject whether it had led to the development of a roadmap for updating ENISA's CERT methods as was intended. It was not possible to assess the extent to which D5 reached its intended output since none of the interviews where familiar with the publication.

At outcome level, the case study showed that in particular D1 and D3 contributed to the dissemination of good practices regarding cyber security among public and private organisations. D1´s contribution was to provide an opportunity for Member States (public and private stakeholders) to meet and exchange good practices and experiences. In relation to D3, the case study finds that the training material itself is considered "good practice" and that as such D3´s contribution to this outcome is direct and important. It was difficult to assess the contribution of D4 and D5 to the dissemination of good practices, since interviewees were less familiar with these publications. At the same time, the survey provided an indication that a contribution may have been made.

In addition to contributing to the dissemination of good practices, D4 and D5 were also intended to contribute to the outcome "Development of Members States' and EU institutions' capabilities in terms of prevention, detection, analysis and response". For D4, the survey seems to confirm that D4 has contributed to developing capacities in prevention, detection, analysis and response in Member States, while interviewees found it too early to judge since new measures have not yet been put to use (work is still at implementation stage). For D5, the survey findings are stronger and indicate that the publication has developed capabilities, while, regrettably, interviewees were not familiar with the publication.

At result level, the case study found only some tangible evidence showing that WPK 2.1 delivered the intended results. In part, this is due to the limited evidence derived from interviews on D4 and D5. The case study presents the strongest evidence when it comes to the deliverables having contributed to developing sound and implementable strategies to ensure preparedness, response and recovery. When ENISA contributes to Member States developing these strategies, it is plausible that the Agency also improves Member States' ability to address cyber challenges, and helps them establish a strategy for how to coordinate and cooperate with private stakeholders during a cyber crisis. In terms of the evidence presented, D1 contributed the most to these results since it helped improve Member States´ NCSS, followed by D3 which is suggested to have improved the capabilities of stakeholders.

And overall inhibitor of ENISA´s ability to deliver these results was that the visibility of the Agency´s activities and publications should be improved.

[Text - Do not delete the following line since it contains a section break. NOTE! Page numbers are updated on "Save" and "Print"]

APPENDIX 1
INTERVIEW GUIDE

Interview Guide for case study WPK 2.1.

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 2.1. 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.

Link in the intervention logic	Interview questions	Interview notes
1. Through its deliverables, WPK 2.1.supports the dissemination of good practices regarding cyber security among public and private organisations	**How would you describe the overall achievements of WPK 2.1[20] when it comes to supporting and advising Member States on the establishment and evaluation of National Cyber Security Strategies?** Is the picture different or similar if you look at the public and private sector?	
2. Through its deliverables WPK 2.1. develops Member States' and EU institutions' capabilities in terms of prevention, detection, analysis and response.	**WPK 2.1. was intended to help build capacity throughout Europe (in terms of cyber security) How would you describe the WPK achievements in this regard?** Who benefitted from this? What was the most/least effective that ENISA did?	
3. **WPK2.1-D1:** Support and advise to Member States on the establishment and evaluation of National Cyber Security Strategies leads to Member States receiving support and advise	*Note: Remember to cross-check with survey responses once the result is available!* **Are you aware of any ENISA activities which support this goal?** **Have you heard of the workshop which took place in September 2016?[21]**	

[20] The WPK terminology will only be used in cases where the interviewee is familiar with it, and in this case Unit COD2. Otherwise, "WPK 3.3." is replaced by the "the Agency" or "ENISA".
[2121] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2015/cyber-security-strategies-critical-information-infrastructures-protection-and-ics-scada-event

Link in the intervention logic	Interview questions	Interview notes
on development and implementation of NCSS (*output*).	Did you take part? Why/Why not? Did anyone you work with take part? **If yes**, *(he/she took part)* how was it useful to you? Can you provide an example? Could something have been improved? **Do you use ENISA's recommendations and good practices on National Cyber Security Strategies? Why/why not?**	
4. WPK2.1-D1: Support and advice on development and implementation of NCSS (*output*) leads the dissemination of good practices regarding cyber security among public and private organisations (*outcome*).	[If the interviewee assesses that Member States have received support and advice from ENISA on development and implementation of NCSS] **In your opinion and experience, what where the effects of this advice and support?** **In your opinion, did it influence the dissemination of good practices related to cyber security?** Can you provide an example? Could something have been improved?	
5. WPK 2.1 –D3: Maintain CERT good practices and training library leads to maintaining and further developing good practices in different areas of capacity building (*output*).	*Note: Remember to cross-check with survey responses once the result is available!* **Are you familiar with any relevant ENISA´s publications?** A. "Mobile Threats Incident Handling. Handbook, Document for teachers"[22] B. "Introduction to advanced artefact analysis. Handbook, Document for teachers[23]" C. "Advanced dynamic analysis. Handbook, Document For Teachers"[24] D. "Advanced static analysis. Handbook, Document for teachers"[25] **If yes,** could you tell me why and how you have used it/them? What did you learn from this publication? In your opinion, did it help maintain or further develop good practices?	

[22] https://www.enisa.europa.eu/activities/cert/support/exercise/files/Mobileincidenthandlinghandbook.pdf
[23] https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/introduction-to-advanced-artefact-analysis.pdf
[24] https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/dynamic-analysis-of-artefacts-handbook.pdf
[25] https://www.enisa.europa.eu/activities/cert/training/training-resources/documents/static-analysis-of-artefacts-handbook.pdf

Link in the intervention logic	Interview questions	Interview notes
	If no, could you explain why you do not use such ENISA publications? Can you provide an example? Could something have been improved?	
6. WPK 2.1– D3: Maintaining and further developing good practices in different areas of capacity building (*output*) leads to the dissemination of good practices regarding cyber security among public and private organisations	[If the interviewee assesses that good practices have been further developed or maintained] **In your opinion and experience, what where the effects of this this (i.e. the maintenance/development of good practices in the area of capacity building?** **In your opinion, did it influence the dissemination of good practices related to cyber security?** Can you provide an example? Could something have been improved?	
7. WPK 2.1 –D4: Building upon the evaluation, ENISA's methods in CERT capacity building are updated and a roadmap is proposed leads to the development of a roadmap for updating ENISA's CERT methods (*output*).	**Are you aware of any update of ENISA´s methods in CERT capacity building** (e.g. the publication "Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations[26]")? **If yes,** could you explain what this update has achieve? Has is built capacity? If yes, how? **To your knowledge, has it led to the development of a roadmap for updating ENISA´s CERT Methods?** **If no,** do you think that updating CERT methods is a priority for ENISA? Could you elaborate?	
8. WPK 2.1 –D4: The development of a roadmap for updating ENISA´s CERT methods *(output)* leads to developing Member States' and EU institutions' capabilities in terms of prevention, detection, analysis and response *(outcome)*	***OUTCOME no 1.*** [If the interviewee assesses that a roadmap has been developed] **In your opinion and experience, what have been/or will be the effects of this** (i.e. the development of a road map for updating ENISA´s CERT Methods)? Have you seen any changes in Member States´ or EU institutions´ capabilities? **In your opinion, has capability in terms of prevention, detection, analysis and/or response been developed?**	

[26] https://www.enisa.europa.eu/activities/cert/support/vulnerability-disclosure

Link in the intervention logic	Interview questions	Interview notes
	Could you provide an example?	
9. WPK 2.1 –D4: The development of a roadmap for updating ENISA´s CERT methods *(output)* leads to the dissemination of good practices regarding cyber security among public and private organisations (outcome)	***OUTCOME no 2.*** *NB: Continued from above, so if the respondent has already pointed to the dissemination of good cyber security practices among private or public stakeholders then skip this question.* [If the interviewee assesses that a roadmap has been developed**] In your opinion and experience, what have been/or will be the effects of this** (i.e. the development of a road map for updating ENISA´s CERT Methods)? Have you seen any changes in cyber security practices amongst private and/or public stakeholders? **In your opinion, have good practices on cyber security practices been disseminated?** Could you provide an example?	
10. WPK 2.1 –D5: Impact evaluations on the usefulness of the ENISA guidelines on capacity building leads to assessments of (the success of) past measures and documents, which supports the development of ENISA Work Programmes in the coming years (output)	**Are you aware of any update of ENISA´s guidelines on CERT capacity building** (e.g. the publication "Leading the way. ENISA's CSIRT-related capacity building activities. Impact Analysis – Update 2015")? **If yes,** could you explain what you thought of this update? **To your knowledge has it helped assess how successful past measures were? If yes, how?** **To your knowledge, has it influenced the development of ENISA´s work Programme(s)?** **If no,** which factors should influence the development of ENISA´s work programme? Could you elaborate?	
11. WPK 2.1 –D5: Developing the ENISA work programmes based on assessments of (the success of) past measures and documents *(output)* **leads to developing Member States' and EU**	***OUTCOME no. 1*** *NB: Continued from above, so if the respondent has already pointed to the development of Member States' and EU institutions' capabilities in terms of prevention, detection, analysis and response then skip this question.* [If the interviewee assesses that assessments of past measures have	

Link in the intervention logic	Interview questions	Interview notes
institutions' capabilities in terms of prevention, detection, analysis and response *(outcome)*	been used to develop ENISA Work programme(s)] **In your opinion and experience, what have been/or will be the effects of this?** **Have you seen any changes in Member States´ or EU institutions´ capabilities?** In your opinion, has capability in terms of prevention, detection, analysis and/or response been developed? Could you provide an example?	
12. WPK 2.1 –D5: Developing the ENISA Work programmes based on assessments of (the success of) past measures and documents *(output)* leads to the dissemination of good practices regarding cyber security among public and private organisations (outcome)	***OUTCOME no. 2*** *NB: Continued from above, so if the respondent has already pointed to the dissemination of good cyber security practices among private or public stakeholders then skip this question.* [If the interviewee assesses that assessments of past measures have been used to develop ENISA Work programme(s)] **In your opinion and experience, what have been/or will be the effects of this** (i.e. using evidence from evaluations/assessments to develop the Work programme(s))? Have you seen any changes in cyber security practices amongst private and/or public stakeholders? **In your opinion, have good practices on cyber security practices been disseminated?** Could you provide an example?	

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

Thank you very much for participating in the interview.