Supporting the CERT Community

"Impact Assessment and Roadmap"

Version 1.0

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Deloitte Bedrijfsrevisoren[1]

Lionel Ferette (ENISA)

Contact

For contacting the authors please use cert-relations@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

As this document is essentially a review of ENISA's work, it has been written by authors outside ENISA. Nevertheless, the authors gratefully acknowledge the continuous support and valuable feedback from Lionel Ferette, Jo De Muynck and Andrea Dufkova (ENISA).

The authors would also like to thank the experts who took to the time to be interviewed and/or fill out the online surveys, and whose opinions and views have informed many of the findings and suggestions presented in chapters 3 to 5 of this study. A special thanks goes to the members of the Expert Group (Shin Adashi, Andrew Cormack, Robert Jonsson, Lino Santos) who provided input on the draft report and validated the findings and suggestions stemming from the information gathered.

[1] Alexander Cespedes Arkush, Dan Cimpean, Joris Lambrechts, Anna Lauridsen

ISBN 978-92-9204-099-4, doi 10.2824/34500

Executive summary

Europe has seen a sharp rise in the number of national/governmental Computer Emergency Response Teams (n/g CERTs) in the past decade with more than 30 established in 2014. ENISA has been instrumental in building and actively supporting a growing network of n/g CERTs since its inception in 2005. The crucial role of a CERT can be compared to that of a 'fire brigade', serving as the first line of defence when security incidents occur. As such, CERTs are primarily in charge of reactive services, such as detection and incident response, but also of security services, which can comprise alerts, advisory and trainings. Despite their unquestionable importance in the face of an ever-growing number of attacks and incidents, the individual capabilities of the n/g CERTs still vary across Europe. In light of this, ENISA's active involvement in supporting CERTs is and will be of great importance to the EU in the years to come. ENISA already publishes recommendations that aim to level these capabilities, and provides training material in order to help CERTs elevate their capabilities level.

This report represents the outcome of an impact assessment performed by Deloitte of ENISA's support to Computer Emergency Response Teams (CERTs) for the period 2005 until today. The impact assessment has served as a basis for a proposed roadmap to 2020.

The key objectives of the study are to:

- Take stock of ENISA achievements in relation to European CERTs, and in light of relevant policy documents;
- Perform an impact analysis of ENISA's achievements with regard to CERTs and other operational communities;
- Provide a roadmap for the period leading up to 2020 based on the results of the impact analysis.

The study team has assessed the impact of the ENISA support to the CERT community following a dual perspective:

- Policy and regulatory;
- Operational.

The legislative and regulatory persepctive covers the objectives formulated in the ENISA Regulation, the 2013 and 2014 ENISA Work Programmes and specific elements of other relevant acts, such as the Digital Agenda for Europe, the Cybersecurity Strategy of the European Union and the proposed NIS Directive.

The operational perspective includes an assessment of the impact of ENISA CERT support looking at three activity pillars:

- Baseline Capabilities for CERTs;
- Capacity building in sharing good practice and CERT training;
- Supporting the CERTs in better collaboration with Law Enforcement.

Additionally, the objective has also been to measure ENISA's overall impact on the CERT communities, beyond the traditional deliverables produced by the Agency, which are typically published on the ENISA website. Hence, the impact assessment also covers a broader range of ENISA activities and deliverables, including:

- Participation in conferences and events (incl. as speaker);
- Meeting facilitations (between CERTs and other actors);
- Liaising, co-operation and information exchange initiatives.

The study was conducted using a multi-dimensional approach including document reviews, online surveys, one-to-one interviews and a validation workshop with input from key CERT experts.

The intended target audience for this study is primarily the ENISA management and experts, and the CERT community. In addition, the study was conducted for the consideration of the ENISA Management Board members, the European Institutions and decision-making bodies responsible for the CERT policy agenda in the EU Member States.

The main recommendations arising out of the impact assessment have been included in a roadmap to 2020, inlcuding suggestions on concrete actions for ENISA's future CERT support. The roadmap, which was validated by a group of CERT experts, can be summarised in the following key points:

- **Policy perspective**: Based on the EU policies and strategy documents reviewed, it is evident that ENISA's role and impact in this domain is recognised and clearly reflected through the ever increasing scope and authority extended over time to the Agency. In the coming years, ENISA may act as a representative voice for CERTs in the European policy context.
- **Operational perspective:** The familiarity with ENISA's CERT support actions is high among the CERT stakeholders and overall there was a positive view of ENISA's CERT related work. However, awareness was higher among representatives of n/g CERTs than among other CERT communities (i.e. in the private, financial sector, etc.). As for the ENISA trainings, there was an expressed need to keep the baseline capabilities more separate from the capacity building activities as the former should cater to the needs of CERT teams of varied levels of maturity. Suggestions for future actions include a clear separation between supports to "new teams" vs. "advanced teams". This is linked to the request for greater clarity of the required level of prior knowledge needed to participate in different trainings. Regarding ENISA reports, there is a need for more technical topics on the one hand for the practitioners, and more policy-related related reports on the other hand, serving to make the case of the ENISA *raison d'etre* to policy and decision-makers. It was also suggested that ENISA should pick up topics and current trends/threats from the EU Member States and research them in-depth, as well as having them translated into several languages.
- **360° Feed-back:** Key points raised stressed ENISA as the main CERT community connector and facilitator, within and beyond the traditional CERT stakeholder groups. ENISA's credibility as the voice of European CERTs within the EU and internationally was undisputed. Improved channels of information was another key point, requesting ENISA to better disseminate information via its website, related to both its activities, but also to alert the CERT community and other operational communities on current attacks and incidents. ENISA is also called upon to lead the work on compiling information on incidents and threats in a catalogue along with recommendations on how to handle them. The 360° feed-back also included a call for greater harmonisation and common standards among CERTs under the lead and guidance of ENISA.

Table of Contents

Executive summary iv

1 Introduction 1

1.1 Policy Perspective – a Brief Overview 1
1.1.1 Europe's 2020 Strategy 1
1.1.2 A Digital Agenda for Europe 1
1.1.3 ENISA Regulation 1
1.1.4 Cybersecurity Strategy of the European Union 2
1.1.5 Proposed NIS Directive 2

1.2 Operational Perspective 2

1.3 Study Purpose and Objectives 3

1.4 Target Audience 3

1.5 Structure of this document 4

2 Methodology 5

2.1 Definitions 5

2.2 Information Collection 6
2.2.1 Desk Study 6
2.2.2 Online surveys 6
2.2.3 Interviews 7
2.2.4 Web impact analysis 8
2.2.5 Validation Workshop with CERT Expert Group 9

2.3 Stakeholder Categories 9
2.3.1 National Liaison Officers 10
2.3.2 National / Governmental CERTs 10
2.3.3 Other CERTs in EU Member States 10
2.3.4 Non-EU CERTs 10
2.3.5 EU Institutions 10
2.3.6 Member State bodies 10
2.3.7 Public & private stakeholders 10

3 Impact Assessment Outcome - Policy and Regulation Perspective 11

3.1 Digital Agenda for Europe 11

3.2 Cybersecurity Strategy of the European Union 12
3.2.1 Respondent views 13

3.3 Proposed NIS Directive 13
3.3.1 Respondent views 13

3.4 ENISA Regulation 14

3.4.1 Respondent views 14

3.5 ENISA Work Programmes 2013-2014 15
3.5.1 ENISA Work Programme 2013 15
3.5.2 ENISA Work Programme 2014 16
3.5.3 Respondent views 17

3.6 Summary Table of ENISA Impact - Policy and Regulation Perspective 18

4 Impact Assessment Outcome – Operational Perspective 19

4.1 Baseline Capabilities for CERTs 19
4.1.1 Respondent awareness of related activities 19
4.1.2 Respondent appreciation of related activities 20
4.1.3 Perceived weaknesses of related activities 21

4.2 Capacity Building for CERTs 21
4.2.1 Respondent awareness of related activities 22
4.2.2 Respondent appreciation of related activities 22
4.2.3 Perceived weaknesses of related activities 23

4.3 Support for CERT – LEA Cooperation 25
4.3.1 Respondent awareness of related activities 25
4.3.2 Respondent appreciation of related activities 26
4.3.3 Perceived weaknesses of related activities 26

4.4 Summary Table of ENISA Impact - Operational Perspective 27

5 Respondent 360° Feed-Back 28

5.1 Suggestions for Future ENISA CERT Activities 28
5.1.1 Improved communication and enhanced information sharing 28
5.1.2 Harmonisation and Common Standards 29
5.1.3 Compilation of Protection and Detection Methods 29

6 Web Impact Analysis 31

6.1 Scope 31

6.2 Results 31

7 Link with 2009 Survey Results for ENISA CERT-related Activities and Deliverables 33

7.1 Summary of the main results of the 2009 report 33

7.2 Links with the 2014 Research Results 34

8 Conclusions and Draft Roadmap Towards 2020 35

8.1 Overall Conclusions 35

8.2 The Way Ahead: Roadmap for ENISA CERT Support 36

8.3 High-Level Roadmap to 2020 37

Annex – 1 List of Interview Questions 40

Annex – 2 Expert Group Members 42

Annex – 3 Glossary 43

Annex – 4 Bibliography 44

1 Introduction

In the past decade, Europe has seen a sharp rise in the number of national/governmental Computer Emergency Response Teams (n/g CERTs), from a small group of eight established in 2005 to more than thirty in 2014. The crucial role of a CERT can be compared to that of a 'fire brigade' serving as the first line of defence when security incidents occur. As such, CERTs are primarily in charge of reactive services, such as detection and incident response, but also of security services, which can comprise alerts, advisory and trainings. Despite their unquestionable importance in the face of an ever-growing number of attacks and incidents, the individual capabilities of the n/g CERTs still vary across Europe. In light of this, ENISA's active involvement in supporting CERTs is and will be of great importance to the EU in the years to come.

1.1 Policy Perspective – a Brief Overview

One of the objectives of this study is to take stock of ENISA's achievements in relation to European CERTs and in light of relevant policy documents. The following documents have therefore been identified for this purpose:

- Europe's 2020 Strategy [1];
- A Digital Agenda for Europe [2];
- ENISA Regulation [3];
- Cybersecurity Strategy of the European Union [4];
- Proposed NIS Directive [5];
- ENISA Work Programme 2013 and 2014.

1.1.1 Europe's 2020 Strategy

The Europe 2020 Strategy [1] aims to support the EU exit from the crisis and to prepare the European Union's economy for the challenges of the next decade. It sets out a vision to achieve high levels of employment, a low carbon economy, productivity and social cohesion, to be implemented through concrete actions at EU and national levels. This requires ownership at top political level and mobilisation from all actors across Europe. One of the seven flagship initiatives of the Europe 2020 strategy is the Digital Agenda for Europe (DAE) – where ENISA has been assigned a key role.

1.1.2 A Digital Agenda for Europe (DAE)

The DAE defines the key enabling role that the use of ICT will have to play if Europe wants to succeed in its ambitions for 2020. The objective is to chart a course to maximise the social and economic potential of ICT, most notably the Internet: for doing business, working, playing, communicating and expressing ourselves freely.

Key Action 6 of the DAE presents measures aiming at a reinforced and high level NIS Policy, including the modernisation of ENISA, and measures allowing faster reactions in the event of cyber-attacks, including a CERT for the EU institutions.

1.1.3 ENISA Regulation

The new ENISA basic Regulation [6], replaces the prior regulation from 2004 [7], allowing ENISA the scope and authority to make an even bigger difference in protecting Europe's cyberspace.

1.1.4 Cybersecurity Strategy of the European Union

The Cybersecurity Strategy of the EU [4] clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world. It proposes specific actions that can enhance the EU's overall performance. It includes a variety of policy tools and involves different types of actors including the EU institutions, Member States and industry.

The strategy foresees a key role for ENISA in protecting Europe's cyberspace to 'achieving cyber resilience' and to 'develop industrial and technological resources for cybersecurity'.

1.1.5 Proposed NIS Directive

According to the Cybersecurity Strategy of the European Union [4], Network and Information Security (NIS) is of paramount importance to our society and the economy as they are becoming increasingly dependent on information systems. For this reason, the European Commission has proposed a Directive on NIS [5] aiming to 'ensure a high common level of NIS'[2] across Member States and foresees a key role for ENISA in protecting Europe's cyberspace.

1.2 Operational Perspective

A CERT [7] is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches. In order to mitigate risks and minimise the number of required responses, most CERTs also provide preventative and educational services for their constituency.

They issue advisories on vulnerabilities in the software and hardware in use, and also inform the users about exploits and viruses taking advantage of these flaws. This allows the constituents to quickly patch and update their systems.

Over the years CERTs have extended their capacities from being a simple reaction force to a complete security service provider, including preventative services such as alerts, security advisory, training, and security management services.

Having a dedicated IT security team [7] helps an organisation to mitigate and prevent major incidents and helps to protect its valuable assets. Services that a CERT can deliver include reactive services, such as alerts and warnings; incident handling; incident analysis; incident response support, and incident response coordination. In addition, there are proactive services, such as announcements and technology watch. Proactive services aim at preventing incidents through awareness building and training, while reactive services aim at handling incidents and mitigating the resulting damage.

Contributing to the security awareness of the constituents and the general public is a preventive practice with the intention to help generate positive publicity. A main part is to share the lessons learned to contribute to the knowledge of others and enable constituents to get appreciation of what the CERT is doing for them. For peers and technical audience, expert papers are shared or expert sessions are organised.

Exercises are useful for clarifying the roles and actions of parties involved in incident handling. In addition they enable practical understanding of possible scenarios of what could happen or has happened highlighting the lessons learned.

[2] What this means is largely open to interpretation and will be clarified at the implementation stage.

Efficient co-operation between CERTs is essential for mitigating even fairly limited incidents and especially when the scope of an issue is larger. It is a recommended to interact and collaborate with as many peers as possible which works best when both sides benefit from it.

It is very valuable to invest in relationships surrounding the CERT environment of operations, such as:

- Law enforcement;
- Professional organisations involved with security issues;
- Professional organisations outside the security community;
- Other security service providers;
- Regional, local and domestic cooperation between CERTs.

1.3 Study Purpose and Objectives

The purpose of the study is to conduct an impact assessment of ENISA's support to Computer Emergency Response Teams for the period 2005 (when ENISA became operational) until today, and to provide a roadmap for the period until 2020.

In this context, the key objectives are to:

- Take stock of ENISA achievements in relation to European CERTs, and in light of relevant policy documents;
- Perform an impact analysis of ENISA's achievements with regard to CERTs and other operational communities;
- Provide a roadmap for the period leading up to 2020 based on the results of the impact analysis.

Whereas the stocktaking exercise and impact analysis looks at ENISA achievements in the period from 2005 until today, the roadmap is forward looking, providing guidance for the next five years until 2020.

The study focuses on the impact in the following three activity pillars:

- Baseline capabilities for CERTs;
- Capacity building, sharing good practice and CERT training;
- Support CERTs to better collaborate with Law Enforcement.

To the extent possible, the objective has also been to measure ENISA's overall impact on the CERT communities, beyond the traditional deliverables produced by the Agency, which are published on its website. Hence, the impact assessment covers a broader range of ENISA activities and deliverables, including:

- Participation in conferences and events (incl. as speaker);
- Meeting facilitations (between CERTs and other actors);
- Liaising, co-operation and information exchange initiatives.

1.4 Target Audience

The study intends to inform ENISA's decision takers regarding its CERT support activities until 2020. In addition, the study is intended to inform wider policy debates about how to make ENISA an even more valuable partner for n/g CERTs and other relevant stakeholders in Europe and beyond, and to inform those n/g CERTs and stakeholders about ways in which ENISA could support their work in the future. The study is also targeted at policy-makers, managerial staff, and senior experts in n/g CERTs and other competent authorities in the European Union Member States as well as senior EU level officials involved in activities supporting the work of CERTs across Europe.

1.5 Structure of this document

The study consists of several chapters. This introductory **chapter 1**, is followed by **chapter 2**, which outlines the study's qualitative methodological approach that combines a review of documents with online surveys and interviews with key experts in the field.

Chapters 3 and 4 present the findings from the online surveys and the interviews highlighting the ENISA impact based on its support to the CERT community following a dual perspective:

- Legislative and regulatory;
- Operational.

Chapter 3, which covers the legislative and regulatory perspective, offers an examination of ENISA's impact with regard to its CERT support activities. This chapter relies mainly on a desk review of key high-level legal and policy documents, ENISA Work Programmes and other relevant ENISA documents. The desk review is complemented by relevant survey results and input from interviews.

The operational perspective, presented in chapter 4, is primarily based on results from the interviews and the surveys. **Chapter 4** also reports upon views expressed by the respondents regarding the impact of CERT support activities that ENISA currently pursues, highlighting their awareness of these activities, as well as their perceptions of them. Moreover, the chapters highlight CERT support activities ENISA could, according to the respondents, continue to pursue and possibly even expand on in the future. The findings in this chapter are presented following the logic of the ENISA activity pillars; baseline capabilities for CERTs, capacity support for CERTs and support for CERT- LEA cooperation.

In **chapter 5**, a wider range of respondent views and feed-back is captured, providing additional suggestions on possible future ENISA support to the CERT community.

Chapter 6 presents the results from a web-analysis conducted to establish the online impact of a limited number of ENISA CERT reports.

Chapter 7 offers a brief overview of the studies on CERT-related activities and deliverables of ENISA conducted in 2009, with a view on verifying whether there are synergies with the findings from this study.

Chapter 8 concludes the study into CERT support activities and their impact, as well as possible future ENISA CERT support by setting out an indicative roadmap for future ENISA CERT support activities in light of the findings presented in the previous chapters.

2 Methodology

In line with the study's objectives, as outlined in chapter 1, the study is based on a multi-dimensional qualitative methodological approach, including a desk review of the key legal and policy documents, interviews of key experts and online surveys with stakeholders from the CERT community and other impacted groups. In addition to these sources, validation of the findings and conclusions was provided by an Expert Group.

Also, we have included a quantitative element to the study to estimate the online references to of a select number of ENISA deliverables. In the following sections, we present how the information collection for this study was undertaken per dimension or source.

2.1 Definitions

The purpose of this section is to provide the reader with an overview of what is understood, within the framework of this study, by "deliverables", "activities" and "CERT community support":

Deliverables	• Reports and studies • Training guides and exercises • Awareness materials
Activities	• Trainings • Support to the set-up of CERTs • Workshops
CERT community support	• Participation in conferences and events (incl. as speaker) • Meeting facilitations (between CERTs and other actors) • Liaising, co-operation and information exchange initiatives

In order to further facilitate for the reader of what is understood by "deliverables", "activities" and "community support" in the remainder of this report we have added a number of concrete examples. This list of examples is non-exhaustive, but it does display a wide variety of ENISA CERT related actions.

"**Deliverables**" are all materials (reports, studies, training guides and exercises and awareness materials, etc.) that ENISA makes available to the CERT community, either though closed distribution channels or through their website, such as:

- The Baseline Capabilities studies on Building a CERT and Running a CERT [8];
- The ENISA Incident Handling Tools Clearinghouse [9].

Reports and studies on CERT services:

- The Detect, Share, Protect study [10];
- Practical information and guidelines for the process of preparing and issuing alerts, warnings and announcements [11];
- Good practice guide for incident management [12].

Publications on cybercrime:

- Legal Information Sharing [13];
- Good Practice Guide for Addressing NIS Aspects of Cybercrime [14];
- Good Practice Collection for CERTs on the Directive on attacks against information systems [15].

"**Activities**" includes open and closed meetings (by invitation only), trainings, set-up of CERTs, exercises and workshops, etc., such as:

- Annual CERT workshops [16];
- 2014 Honeynet Project Workshop [17];
- ENISA high-level events [16];
- ENISA-EUROPOL/EC3 workshops [16];
- EU FI-ISAC [18];
- EU CERT Community – TF-CSIRT [19];
- Global CERT Community – FIRST [20];
- Trainings, including TRANSITS Trainings [21].

"**Community support**" englobes ENISA activities and deliverables that are of a more *ad hoc* nature and therefore less visible on the ENISA website and through other communication channels, such as:

- Participation in conferences/events (including as speaker/attendee);
- Meeting facilitations (between CERTS and other actors);
- Liaising / raising awareness;
- Proceedings from various roundtables ENISA participated in;
- ENISA visits to CERTs.

2.2 Information Collection

2.2.1 Desk Study

A number of key documents have served as a foundation for the study to establish the legal and policy framework of ENISA's CERT related mandate and performance with regard to supporting the CERTs. The overview below provides a detailed list of all the documents that have been reviewed within the framework of this study:

- Europe 2020 Strategy [1];
- Digital Agenda [2];
- Cybersecurity Strategy of the EU [4];
- Proposed NIS Directive [5];
- ENISA Regulation [6];
- ENISA Work Programme 2013 [22] and 2014 [23].

2.2.2 Online surveys

The primary measurement instrument used for this study was an online survey tool setup by the study team particularly for this study. This web-based questionnaire was published on the SurveyMonkey platform and was supported by appropriate security measures including SSL and certificate technologies. We designed the online survey instrument in order to provide:

- A clear survey structure with a presentation of questions and possible answers;
- An integrated management platform supporting the online survey allowing close monitoring of the survey progress and results.

Selected experts from seven stakeholder groups were contacted to participate in the online survey. The table below presents the response rate per stakeholder group.

Stakeholder group	Number Contacted
A. National Liaison Officers	30 contacted
B. National/Governmental CERTs	50 contacted
C. CERTs in EU Member States (including academic, industry, etc.)	108 contacted
D. Non-EU CERTs	60 contacted
E. European institutions and other bodies (e.g. JRC, EC, CERT-EU etc.)	13 contacted
F. Public and private stakeholders	61 contacted

The number of experts, and their distribution in groups allowed the survey team to have a representative panel of the target audience for ENISA's CERT-related activities, and limit the possibility of biased results.

The study team prepared detailed guidance for the participants of the survey, in order to increase the overall efficiency of the process, and to increase the quality of the collected input. In line with ENISA good practice of the implementation of its activities and procedures, the study team observed the relevant EU regulations [24] [25].

The study team overcame the relatively modest initial response rates for some target categories (mainly Public and Private Stakeholders) by conducting in-depth interviews and by collecting additional qualitative input from the experts (see 2.2.3).

2.2.3 Interviews

The list of respondents interviewed was jointly drawn up by ENISA and the study team. The study team conducted the interviews, either in person (in Brussels and Athens) or via phone, between July and September 2014.

The interviews were pursued in a semi-structured manner allowing for auxiliary questions and for new lines of questioning depending on the responses of the respondents. During the interviews, the study team followed an agreed-upon protocol covering all the different themes that were treated during the interview with the selected CERT stakeholders. However, interview respondents were free to discuss additional relevant topics they considered as important or interesting.

Only note taking was used to capture the content of the interviews. Referencing to Chatham House rules, interviewees were assured of non-attribution and anonymity when using direct quotes, unless they gave the study team explicit permission to be quoted. As a result, in reporting on the interviews in this study, a quasi-anonymous approach is pursued, with references only being made to participant's role or type of host organisation, i.e. CERT, LEA, policy-making body, or other.

Host organisation of the interview respondents include:

It should be noted that respondents interviewed for this study constitute a limited selection of CERT practitioners, policy officers, and other representatives of relevant communities. Even though the greatest possible effort was made to ensure that only leading experts on CERT practices were interviewed, the dataset should therefore not be taken as in any way exhaustive. Rather, evidence generated from the interviews should be interpreted as anecdotal in nature, indicating select expectations and perceptions of ENISA's CERT support work among highly experienced "end-users."

2.2.4 Web impact analysis

As a complement to the desk review, online survey and interviews, a web impact analysis was conducted. The main aim of the web impact analysis was to identify to what extent ENISA CERT related deliverables have been referenced to online, in order to gain insight into what types of environments and stakeholder groups for which these deliverables are relevant or of interest, as to see the quantitative outreach. The scope of the web impact analysis focused exclusively on deliverables published in 2013 and 2014, and the following categories of online sources have been taken into account:

- **News sites or journals**; e.g. www.darkreading.com/ and www.all-about-security.de.
- **Social media**; such as Twitter or Facebook;
- **Blogs**; such as www.infosecsquare.blogsspot.com and http://lamaredugof.fr;
- **Professional associations**; such as www.auditors-censors.com and www.intgovforum.org;
- **Academic papers, articles or reports**; such as the International Electronics Communication - Industry Developments In The Bulletin [26];

Following a review of Google search services available, the operator "allintext" was identified as the most suitable for achieving the purpose of the web impact analysis. The results of this analysis are presented in chapter 6.

2.2.5 Validation Workshop with CERT Expert Group

Following the information collection phase, a workshop was organised on September 12, 2014, in order to validate the research results from the impact assessment and to collect direct input, suggestions and views with regards to the draft roadmap and implementation plan.

The validation workshop focused on the policy and regulation perspective, as well as the CERT operational perspective. The findings were validated by an Expert Group, in close co-ordination with ENISA. The Expert Group was composed by members form the CERT community (see Annex 2).

Overall, the Expert Group was set up to contribute in the following areas:

- Provide input on the European CERT ecosystems, insights into both the policy and operation levels, throughout the project;
- Participation at a workshop with ENISA on the impact assessment outcome focus on the policy and regulation perspective;
- Attend the ENISA seminar for presentation of the project outcomes.

The validation of the Expert Group has been included in chapters 3-5. Additionally, our findings were supported by another recent study into ENISA's CERT support activities produced by RAND Europe and time.lex [27].

2.3 Stakeholder Categories

The stakeholders were grouped in line with the Cybersecurity Strategy of the European Union [4]. In addition, we added an international layer to it in order to capture how ENISA is perceived outside of the European Union. In the sections below, we provide brief information on each of the different stakeholder groups to provide the reader with a deeper understanding of the players behind the findings of this report.

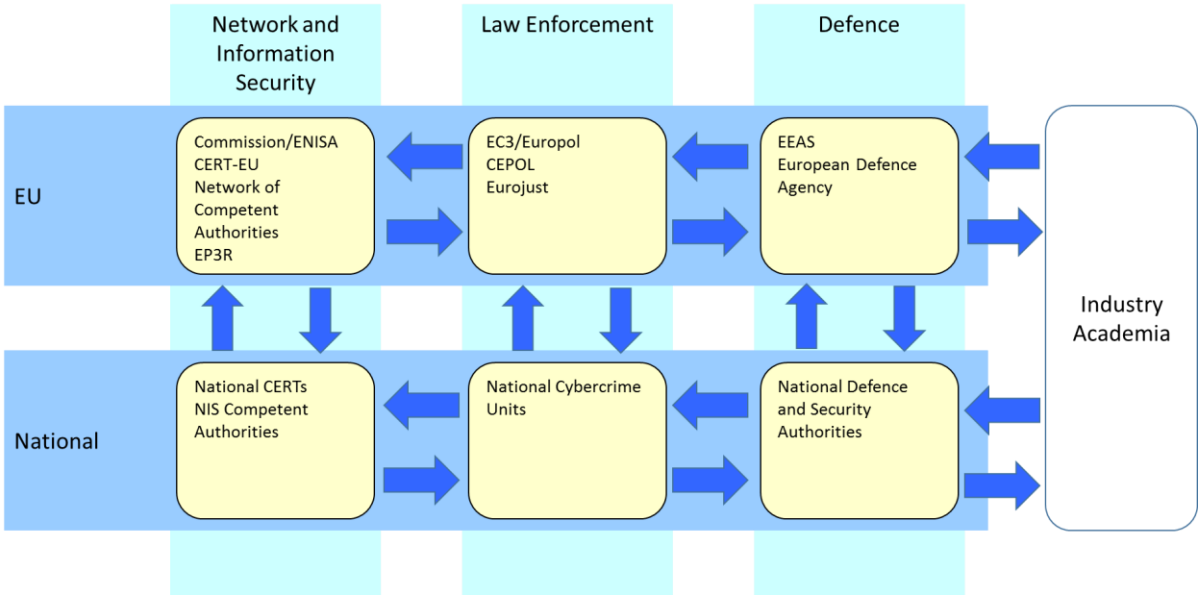


Figure 1 - Roles and Responsibilities

(source: the Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union)

2.3.1 National Liaison Officers

ENISA has set up a network of National Liaison Officers (NLOs), which serve as ENISA's point of reference into the Member States on specific issues. ENISA also gains access to a network of national contacts through individual NLOs, reinforcing the activity of the Agency in the Member States.

Member States representatives - one from each EU and EEA country - are part of the NLO network. A representative from the European Commission and a representative from the Council of the European Union are also part of this network.

2.3.2 National / Governmental CERTs

National/governmental CERTs (n/g CERTs) are Computer Emergency Response Teams that serve the government of a country by helping to protect the critical information infrastructure. N/g CERTs play a key role in coordinating incident management with the relevant stakeholders at the national level. They also bear the responsibility for cooperation with the national and governmental teams in other countries. Examples include CERT-Bund (Bundesverwaltung), NCERT-GR and CERT-Hungary.

2.3.3 Other CERTs in EU Member States

This stakeholder group represents CERTs which are located in the European Union but not mandated by the government. Examples include among others CERTs in research and education, as well as military CERTs.

2.3.4 Non-EU CERTs

This stakeholder group represents CERTs which are located outside of the European Union. Examples include ICANN CIRT (Internet Corporation for Assigned Names and Numbers), ILAN CERT Israeli Academic) and Incita Security CERT.

2.3.5 EU Institutions

The institutions of the European Union include the European Commission, the European Parliament and related Agencies, such as the JRC and CERT-EU. Examples of this stakeholder group include regulators, policy makers and other public bodies.

2.3.6 Member State bodies

This stakeholder group includes leaders that represent a country within an international organisation that is related to CERT activities or information security in the broader term. Examples include, NIS and cyber-security bodies.

2.3.7 Public & private stakeholders

This group includes any other public or private organisation that relates to CERT activities. Examples include professional services, associations of providers and legal & policy experts.

3 Impact Assessment Outcome - Policy and Regulation Perspective

This chapter presents an overview of the results of the desk review, which was undertaken focusing on key strategic documents outlining the EUs policies influencing the domain, as well as the main official documents laying down ENISA's mandate and tasks related to support to CERTs. Additionally, views of respondents of both the interviews and surveys with regard to the policy and regulation perspective of ENISA's support activities have been incorporated where applicable. The information gathered has been grouped according to the following structure:

- Digital Agenda for Europe [2];
- Cybersecurity Strategy of the European Union [4];
- Proposed NIS directive [5];
- ENISA Regulation [6];
- ENISA Work Programmes 2013 [22] and 2014[3] [28].

3.1 Digital Agenda for Europe

One of the seven flagship initiatives of the Europe 2020 Strategy for smart growth is the Digital Agenda for Europe [2] where ENISA has been assigned a key role. The DAE defines the key enabling role that the use of Information and Communication Technologies will have to play if Europe wants to succeed in its ambitions for 2020.

The DAE frames its key actions around the need to tackle seven problem areas linked to the three growth dimensions set out in Europe 2020. One of these problem areas relevant to the role of ENISA is 'rising cybercrime and risk of low trust in networks'.

These problem areas are translated into corresponding action areas. Under the "trust and security" action area, cooperation of relevant actors needs to be organised at a global level to be effectively able to fight and mitigate security threats. Each action area describes corresponding legislative actions and proposals. These are:

- A vibrant digital single market;
- Interoperability and standards;
- **Trust and security;**
- Fast and ultrafast Internet access;
- Research and innovation;
- Enhancing digital literacy and skills; and
- ICT-enabled benefits for EU society.

[3] Previous Work Programmes are not included in this study because 2013 was the first year ENISA had a structured and dedicated CERT Support Team

According to the DAE, European citizens see the lack of security and trust as a major barrier to the widespread uptake of ICTs. The most relevant policy areas in this regard are:

- Network and Information Security (NIS); and
- The fight against cybercrime.

CERT related recommendations in the DAE mainly focus on action points for the European Commission and Member States. For example, under the third pillar "Trust and Security", the DAE proposes that a wider network of CERTs and a CERT for the European institutions be established. In addition, the DAE indicates the necessity to promote cooperation between CERTs and LEAs together with the establishment of a system of contact points to assist in the prevention of cybercrime and response to cyber-attacks. However, it is not specified whether responses to cyber-attacks encompass technical or non-technical responses.

Other proposed initiatives related to CERT activities include the establishment of large-scale attack simulations and practice mitigation strategies and cybercrime related reporting and alert platforms. The DAE also indicates that the Commission should propose a regulation to modernise ENISA.

3.2 Cybersecurity Strategy of the European Union

The Cybersecurity Strategy of the European Union [4] outlines the EU's vision in the domain of cyber security, clarifying roles and responsibilities, and specifying required actions to promote online security and citizens' rights.

The vision presented in the Strategy is articulated in five priorities and foresees a key role for ENISA in protecting Europe's cyberspace in the first and the forth priority to "achieving cyber resilience" and to "develop industrial and technological resources for cybersecurity". ENISA also has an implicit role in the second and fifth priorities to "drastically reduce cybercrime" and "develop the industrial and technological resources for cybersecurity".

To boost cyber resilience in the EU, both the public and the private sector must develop capabilities and cooperate effectively. In the second priority of the Strategy the Commission asks ENISA to:

- Assist Member States in developing strong national cyber resilience capabilities, by building expertise on security and resilience of industrial control systems, transport and energy infrastructure;
- Examine in 2013 the feasibility of Computer Security Incident Response Team(s) for Industrial Control Systems (ICS-CSIRTs) for the EU;
- Continue supporting the MS and the EU institutions in carrying out regular pan-European cyber incident exercises which will also constitute the operational basis for the EU participation in international cyber incident exercises.

To develop industrial and technological resources for cybersecurity, in the fourth priority of the Strategy the Commission asks ENISA to:

- Propose in 2013 a roadmap for a 'Network and Information Security driving licence' as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators);
- Develop, in cooperation with relevant national competent authorities, relevant stakeholders, and international and European standardisation bodies and the European Commission Joint Research Centre, technical guidelines and recommendations for the adoption of NIS standards and good practices in the public and private sectors.

The Cybersecurity Strategy of the European Union is not a legally binding document, however ENISA is expected to take into account these requests coming from such a high level document.

3.2.1 Respondent views

Respondents indicate that ENISA CERT activities are important in supporting the Cybersecurity Strategy of the European Union, in particular the goals related to co-ordination between NIS competent authorities, CERTs, Law Enforcement Agencies and defence. Concerning the current focus areas and activities of ENISA in the area of CERTs and operational communities, respondents were of the opinion that in line with the Cybersecurity Strategy of the ENISA should among others:

- Assist in the creation of cross-border operational procedures and crisis management processes; together with technical guidelines and recommendations for national cyber resilience capabilities.
- Develop and promote models of cooperation which have a good balance between declared level of responses or provided (voluntary) services; mandatory obligations (e.g. NIS directive, telecom package); Incentives for cooperation in the form of tangible benefits;
- Enable national CERTS to support other CERTs in the different industries such as finance, and CIIP by promoting the increase of support from the ministry level for which ENISA could assist in raising awareness on this strategic level.
- Improve the capacity and tools available for the national CERT level, especially in the field of critical infrastructures. ENISA should promote and support (financially) joined tools used between CERTs in Europe.

3.3 Proposed NIS Directive

The NIS Directive is a legislative instrument to support the achievement of some of the high level goals identified in the Cybersecurity Strategy, including promoting a high common level of NIS by improving internet security, private networks, and information systems. The proposed NIS Directive [5] lays down measures to ensure a high common level of Network and Information Security (NIS) across the European Union:

- Establish common minimum requirements for NIS at national level;
- Set up coordinated prevention, detection mitigation and response mechanism, enabling information sharing and mutual assistance amongst the national NIS competent authorities;
- Improve preparedness and engagement of the private sector.

The proposed NIS Directive elaborates on the role of ENISA with regard to supporting Member States and the EU by assisting in the operation of the cooperation network, providing Member States and the EU with its expertise and advice, and by facilitating the exchange of best practices. The proposal also suggests that ENISA should cooperate with the EU institutions and Member States to develop a cooperation plan to counter risks and incidents.

3.3.1 Respondent views

Respondents generally are of the opinion that ENISA should be facilitating, and encouraging information exchange as described in article 8 of the proposed NIS Directive as opposed to simply being nominated as a Single Point of Contact (SPOC) which would not be a guarantee for information exchange.

3.4 ENISA Regulation

The new ENISA Regulation [6], constitutes the most recent ENISA mandate and replaces the prior Regulation from 2004 [7]. It guarantees the operations of ENISA until 2018 and provides the Agency's general strategy, building on ENISA's achievements in areas such as support to CERTs in Member States and facilitation of pan-European cybersecurity exercises.

The new Regulation enlarges the scope of ENISA and its authority to make an even bigger difference in protecting Europe's cyberspace, including ENISA supporting the development of EU cybersecurity policy and legislation. In terms of ENISA CERT support activities, the Regulation lays down a number of expectations in relation to n/g CERTs and other CERTs in Europe, which are summarised below.

- **CERT Operational Frameworks and Mandates**: Facilitation of the emergence and maintenance of a stable n/g CERT architecture across the EU, which also provides overarching framework for EU information security.
- **CERT Service Portfolios**: ENISA support to the formulation of a peer review system amongst n/g CERTs to assess CERT performance against a common set of capabilities.
- **CERT Resources**: ENISA support for strengthened capabilities of n/g CERTs that should also establish a common set of operational capability criteria for n/g CERTs. These should also match those of the 'most developed CERTs' in the EU.
- **Cooperation**: The Regulation tasks ENISA to "promote cooperation and the exchange of information and best practices' between CERTs and other relevant organisations", and also gives ENISA a greater interfacing ability with the European Cybercrime Centre, providing for a more proactive ENISA role with regard to encouraging information exchange amongst n/g CERTs and LEAs.

3.4.1 Respondent views

From the expressed respondent views, ENISA is considered to have been successful in achieving the objectives outlined in the ENISA Regulation as concerns its support to CERTs in EU Member States. However, certain respondents were of the opinion that ENISA should concentrate more on the tasks in its mandate, as opposed to providing what was called "ad hoc suggestions"[4].

Most respondents are of the opinion that the current strategic objectives of ENISA are sufficiently relevant. In addition, respondents voiced the following views and suggestions:

- It is apparent that the structure of ENISA is still evolving, which is the case for the cyber security area at large (apart from the private sector). The current ENISA objectives are sufficient, but there is still room for improvement.
- CERTs often work at very deep technical research level, however, ENISA is more concentrating on strategic and operational level activities.
- ENISA should increase the support of the operational CERT teams and especially help them to reduce the legal uncertainty with data and information exchange.

[4] Unfortunately, time constraints prevented to go into more details or examples.

3.5 ENISA Work Programmes 2013-2014

3.5.1 ENISA Work Programme 2013

The 2013 ENISA Work Programme [28] set out three core operational work streams (WS) for ENISA during 2013, which were concerned with:

- WS1: Evolving risk environment and opportunities;
- WS2: Improving pan-European CIIP and resilience;
- WS3: Enabling communities to improve NIS.

Globally, these work streams represented a continuation of the work ENISA had carried out the previous year, taking on board the changed priority and focus set out by the ENISA Management Board. The three work streams reflect the evolution of the global threat environment, including the need to continuously improve Critical Infrastructure Protection (CIIP) in the EU, as well as the need to support the CERT and other operational communities.

The desk review concluded that there were two work packages, both under WS3, which directly outlined ENISA CERT support activities, as described below.

The overall objectives of WS3, linked to CERT support, include to:

- Keep up to date with and enhance the operational capabilities of MS institutions by helping the CERT community to increase its support to law enforcement, the fight against cyber-crime, etc;
- Support and enhance co-operation between CERTs and other communities.

3.5.1.1 Work Package 3.1: Application of Good Practice for CERTs

The desired impact of the work package 3.1 aimed at improving:

- The communication and information exchange between n/g CERTs and other MS bodies;
- The operational practices of n/g CERTs;
- The collaboration capabilities of n/g CERTs.

The aim of the work package was set out to be achieved through the set-up of a platform for the safe interaction and interchange of information between European n/g CERTs; the deployment of the European Information Sharing & Alert System; a good practice guide on Alerts, Warnings and Announcements, as well as through a CERT inventory.

3.5.1.2 Work Package 3.2: Enabling Collaborative Communities

The desired impact of the work package 3.2 aimed at:

- Improving the operational capabilities of n/g CERTs;
- Assisting Member States in identifying and removing possible legal barriers to information sharing concerning n/g CERTs baseline capabilities efficiency;
- Improving pan-European cooperation between CERTs and LEAs in the fight against cybercrime.

To meet these objectives, ENISA was requested to produce a good practice guide on the practical implementation of the Directive 2013/40/EU on Attacks against Information Systems, as well as a good practice guide on the harmonisation and implementation of legal frameworks for information sharing and international incident handling processes. ENISA was also expected to widely disseminate CERT exercise material on cybercrime scenarios and to manage the 8th Annual CERT workshop on the legal perspective and operational aspects of international incident handling. ENISA was further tasked to perform CERT training support activities to ensure that those trained are introduced to CERT and other

stakeholder communities involved in incident response. ENISA was also requested to develop a new version of the Baseline capabilities framework, including international harmonisation and appropriate ICS-CERT capabilities.

3.5.2 ENISA Work Programme 2014

The 2014 Work Programme [23] stressed that ENISA's strategic priorities are designed to support Member States' efforts to meet EU policy objectives. The Work Programme reflects the fact that ENISA obtained new tasks to perform during 2014 following its new mandate and the Cybersecurity Strategy for the European Union. In this context, ENISA has identified three Work Streams that define ENISA's current core operational activities:

- WS1: Support EU policy building;
- WS2: Support capacity building;
- WS3: Support cooperation.

As was the case in 2013, not all work streams included CERT related tasks for ENISA, and therefore the desk review focused on work packages two and three as described below.

3.5.2.1 Work Package 2.1: Support Member States' Capacity Building

Work Package 2.1 aims at improving the operational activities of CERTs through the following:

- Stock-taking of achievements, good practices and experience with a view to develop a road map;
- Enhance training and exercise methodology to improve the competencies of trainers;
- Produce good practice guides on training methodologies for CERTs derived from experiences in delivering suitable CERT training;
- Provide an update of the "baseline capabilities" definition and to draw conclusions for new training materials. In addition, ENISA will deliver a new set of CERT exercise material with at least five new scenarios covering the four main baseline capabilities competencies, including operational, technical, mandate and cooperation competencies.

3.5.2.2 Work Package 3.3: Regular Cooperation among NIS Communities

As part of WS3, ENISA implements Work Package 3.3, aims at enabling ENISA to:

- Actively support or organise common trainings for different communities, such as CERTs and LEAs;
- Engage with the European Cyber Crime Centre (EC3), where appropriate, through formal and informal cooperation channels;
- Take stock of the response of other communities to cyber security challenges and establish how they could inform the works of CERTs;
- Facilitate the outreach to other bodies and /or communities, including taking stock of accepted methods for trust building within and among communities;
- Continue to collect good practice useful for CERTs and LEAs and to enhance ENISA exercise and training materials.

This work package extends the scope of ENISA's support to the communities dealing with NIS to non-operational communities, to enable communications between CERTs, law enforcement, financial and other communities. Activities scheduled to implement these goals include ENISA to utilise the 9th ENISA CERT workshop to prepare future work in the area of CERT training and CERT cooperation with LEA s in collaboration with the European Cybercrime Centre (EC3). ENISA will also engage in the formulation

of a good practice guide and/or training and exercise materials concerning the exchange and processing of actionable information by CERTs, as well as in the drafting of good practice materials for first responders in cooperation with the EC3. Moreover, ENISA will prepare draft reports on "stocktaking on channels and formats for exchange of operational information", as well as on "scalable and accepted methods for trust building within and among communities" [23].

3.5.3 Respondent views

Globally, most of the survey respondents agree that ENISA has successfully implemented the CERT related activities set out in the past annual Work Programmes.

One respondent stated that ENISA has created an informal network of CERTs, but also in the private sector, which provide added value to the CERTs in terms of informal knowledge and practices. The same respondent also pointed out that while these networks are great for CERTs from smaller Member States, with lesser resources at their disposal, the CERTs from bigger Member States tend to hold back when it comes to information sharing.

One perceived issue with the ENISA annual Work Programmes, which is also related to the fast and ever changing environment that the Agency works in, is the need to fulfil targets that were set one to two years in advance regardless of the attacks or incidents that may occur in the meantime. From the respondent views, it was clear that there is an understanding that the ENISA resources are limited and that it is hard to constantly work on things as they come up to the detriment of pre-established work programmes.

Generally, awareness of ENISA's CERT support actions was high among almost all of the interviews and survey respondents, and there was overall a positive view of the work ENISA was performing to support CERTs. As for the consumption of ENISA's products and services, it seems to be driven by demand rather than supply, suggesting that ENISA should both survey and shape demand. Thus, it was suggested that less mature n/g CERTs often required higher levels of awareness raising about areas for improving their capacities and the products and services ENISA offers in this respect. Similarly, respondents repeatedly highlighted ENISA's role as a facilitator of exchange among different communities, in line with its support to strengthening CERT cooperation with other actors,

Respondents repeatedly made the comment that ENISA was generally focusing on the right issues and that it was doing what it should be doing in the context of its mandate. One respondent commented that ENISA understood the CERT world and the requirements of the community very well and that, despite its limited resources, ENISA filled a gap in establishing momentum that the community could not sustain on its own. However, one respondent remarked that very often boundaries between what constituted training and capacity building became unclear.

One respondent noted that ENISA was not an operational agency, as opposed to the community it aimed to support, which, at times, resulted in a disconnect between the two. Generally, it was noted that gaps with regard to incident response handling were gaps ENISA could not easily bridge, due to the remits of its mandate. However, as another expert suggested, these gaps might be bridged if ENISA were to assist in the establishment of national NIS strategies

3.6 Summary Table of ENISA Impact - Policy and Regulation Perspective

The ENISA impact in the area of CERT support from a policy and regulation perspective was determined based on the evolution since 2010 (Digital Agenda for Europe) and increase of proposed CERT related activities throughout the policy documents in scope of the desk review. This increase in active CERT involvement, suggests a strong recognition of ENISA's past activities and the need for further involvement.

Relevant Policy	Level of Impact	Proposed ENISA CERT related activities	Conclusion
Digital Agenda for Europe	**Medium**	The DAE proposes: • A wider network of CERTs; • CERT/LEA cooperation; • Large-scale attack simulations; • Practice mitigation strategies; • Cybercrime related reporting and alert platforms.	ENISA's achievements in supporting CERTs in MS and facilitating pan-EU cybersecurity exercises are recognised. The DAE proposed to modernise ENISA.
ENISA Regulation	**High**	Mandates ENISA to: • Support the development of EU cybersecurity policy and legislation; • Support CERT Operational Frameworks and Mandates, CERT Service Portfolios, CERT Resources and cooperation.	The scope and authority of ENISA is strengthened to involve the Agency increasingly in protecting the European cyberspace.
Cybersecurity Strategy of the EU	**Medium**	The Commission asks ENISA to: • Assist MS in developing cyber resilience capabilities; • Examine the feasibility of ICS-CSIRTs; • Continue supporting pan-EU cyber incident exercices ; • Propose a roadmap for a 'NIS driving licence'; • Develop technical guidelines and recommendations.	ENISA is considered as a key actor in achieving cyber resilience and develop industrial and technological resources for cybersecurity.
Proposed[5] NIS Directive	**High**	The Commission would task ENISA to: • Assist in the operation of the cooperation network; • Provide MS and the EU with expertise and advice; • Facilitate the exchange of best practices.	ENISAs role as a key actor in achieving cyber resilience and develop resources for cybersecurity is reinforced in line with the priorities of the Cybersecurity Strategy of the European Union.

[5] At the time of writing, adoption of the NIS Directive is pending. However, no significant changes are expected to the proposed directive.

4 Impact Assessment Outcome – Operational Perspective

This chapter reports upon the views of both the interview and survey respondents with regard to the operational perspective of ENISA support activities focusing on the development of baseline capabilities for CERTs, CERT capacity building and collaboration between CERTs and LEAs. The information and views gathered have been grouped into three overarching themes:

- Respondent awareness of related activities;
- Respondent appreciation of related activities;
- Perceived weaknesses of related activities.

In addition to filling out the online surveys and during the interviews, several respondents also shared their views on possible future activities of ENISA in the area of support to CERTs, which are included in this chapter.

4.1 Baseline Capabilities for CERTs

"ENISA's goal is to continuously support the Member States in enhancing and strengthening the cooperation among n/g CERTs in order to achieve a powerful incident response when it is needed"[6].

ENISA has identified four baseline capabilities to focus on for its research and continuous work to support CERTs: mandate and strategy, service portfolio, operational and cooperation capabilities. These baseline capabilities aim to tackle the diversity of capabilities across Member States, which is seen by ENISA as the main obstacle to cross-border cooperation and incident response. To this end, ENISA has produced a number of documents that constitute an initial minimum set of capabilities that a CERT in charge of protecting critical information infrastructure (CIIP) in the Member States should possess to take part and contribute to a sustainable cross-border information sharing and cooperation.

4.1.1 Respondent awareness of related activities

The ENISA baseline capability guides were well known among the respondents, regardless of stakeholder group and position within the organisation. This is evident from the high response rate across the board and from the generally positive feed-back on the guides and their usefulness as described below. The baseline capability guides were clearly 'on the radar screen' [27] of end-users, even though they had not read all of them. A majority of the respondents claimed that, depending on their information needs, ENISA was one of the primary, if not the main source of CERT related information. However, they would generally turn to other sites for updates on the most recent attacks and incidents.

Indeed, several of the respondents referred to their participation in the preparation or production of the various materials as a reason their familiarity with these [27]. However, among the newer CERTs, it was common to use the ENISA baseline capability guides as a part of the day to day business.

[6] https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

It is important to highlight that broad familiarisation with the CERT baseline capabilities guides, and of ENISA CERT activities at large, was generally lower in other operational communities, such as the private sector.

4.1.2 Respondent appreciation of related activities

Overall, ENISA's baseline capabilities guides and tools were much appreciated by the respondents. From the surveys, we conclude that the general perception of ENISA CERT baseline capabilities materials have a high quality. The respondents state that the reports are well written and structured, that they meet their objectives and that they are sufficiently comprehensive (relevant facts and accurate conclusions). The guides were also greatly appreciated for their good description of necessary operational capabilities and opportunities to strengthen cooperation with other stakeholders [27]. Several respondents stressed ENISA's omnipresence in the European CERT environment, especially with a view to the ENISA staff presence at events and conferences, but also in terms of their accessibility. ENISA was appreciated for being "active and reactive" in developing relationships between CERTs and even actors from the EU institutions. Face to face interaction and networking was particularly appreciated, although respondents also wondered how ENISA finds time to do other work in between conferences and travel. One suggestion was to create account management practices where one ENISA staff would be responsible for a number of EU Member States so as to limit the amount of travel. The respondent also realised that this might be difficult to translate into reality in light of ENISA's limited number of personnel.

Many respondents attested to the benefits of using the ENISA good practice guides when building up their CERT capabilities from scratch. For instance, a number of respondents also commented that they had provided the ENISA baseline capability guides as a "starter kit" to new CERTs, including other non-n/g CERTs, both in the EU and beyond [27]. Similarly, a few participants noted that they had used ENISA's good practice guides when they established their local CERT team, although this was not universally reported and seemed to differ depending upon the size and resources available to CERTs.

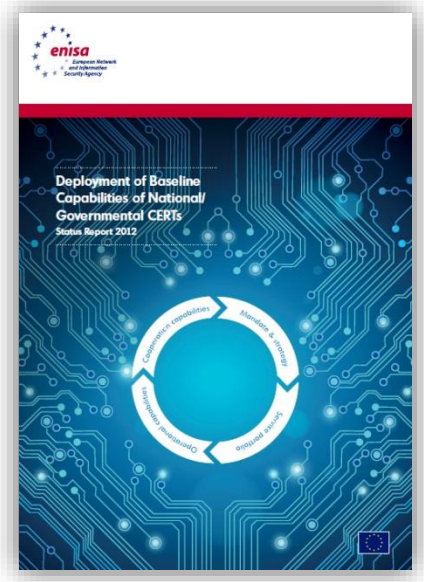
It is interesting to highlight the difference in appreciation of ENISA's good practice guides between newer CERT teams and more mature teams. Representatives of more mature CERTs seemed not to have used the guides as much, even though they still regarded the guides as a useful resource for "checking certain things" [27]. Along these lines, a CERT representative mentioned that his team usually turned to the baseline capabilities guide when considering process improvements or change management. Another respondent expressed appreciation over the ENISA website and the separation between open and closed parts, which was seen as valuable for building trust in the community.

One specific strength of the reports, as they summarise a set of issues that affected CERTs, was their potential for serving other purposes, for instance in the formulation of a national cyber security strategies [27].

An unexpected strength of the baseline capabilities was their prospective ability to act as a tool for "regulating" [27] the CERT community, or indeed to act as an indirect mechanism supporting certification, and in the long-run greater harmonisation. However, when it comes to the needs to the CERTs, there is no "one-size fits all", and hence not all ENISA materials can be equally useful to all CERTs. However, the call for greater harmonisation and standardisation was recurrent among the respondents.

4.1.3 Perceived weaknesses of related activities

A few weaknesses were identified with regard to existing ENISA CERT support activities in the domain of baseline capability building. For one, it was felt that the material needed to be better disseminated. Given the extensive effort in preparing the good practice guides and tools, respondents reported that more could be done to improve awareness about their existence. Some respondents suggested that ENISA released outputs with "little fanfare" [27] and suggested that this could be improved. However, others also suggested that in some cases ENISA could do relatively little about what was seen as a general lack in demand on part of some CERTs or even a lack of interest.



A second criticism that was repeatedly made was that some of ENISA's guides were too long and that they could be made much more concise, while also featuring an accompanying short summary report or a checklist. In this respect, it was also suggested that greater effort could be made in making the good practice guides more accessible for busy readers, although their utility as a reference work was also recognised [27].

Third, one respondent reported that ENISA's guides could be updated more frequently, while another respondent identified a strength of the reports residing in them encapsulating a set of issues that affected CERTs but which could also be raised to help educate others (e.g. in the formulation of a National Cyber Security Strategy).

Fourth, a weakness was identified with regard to the onward development and embedding of capabilities identified in ENISA's guides. Thus, although the guides were seen as being useful in the formative stages of a CERT's lifecycle [27], respondents argued that it was an outstanding question as to what happened afterward and how ENISA's guides could continue to be useful during the later phases of a CERT's lifecycle. On a similar note, one of the respondents from an EU institution, who expressed strong appreciation of ENISA's work on helping CERTs to improve and mature, suggested that ENISA should have a role in supporting the process of 'spiral of maturity', implying the continued assistance of CERTs including follow-up after the set-up and further maturation, including providing related trainings.

An important point regarding the maturity of CERTs was brought up by some respondents from an n/g CERT. Their point was that ENISA is at times seen as wanting to move "too fast" and interested in moving onto more sophisticated topics at a stage that is too early for the newer CERTs. The respondents were calling for a more distinct difference in terms of pace and focus between the trainings for newer CERTs which are in need of 'new team support', as opposed to "advanced team support". The suggestion of the respondents was for trainings and networking for the newer CERTs to focus on their baseline capabilities in order for them to get up and running.

4.2 Capacity Building for CERTs

ENISA's support for CERTs in terms of capacity building focuses primarily on, but are not limited to, trainings, workshops, exercises and dissemination of good practices. ENISA CERT exercises and training material were introduced in 2008, and in 2012 and 2013 it was complemented with new exercise scenarios containing essential material for success in the CERT community and in the field of information

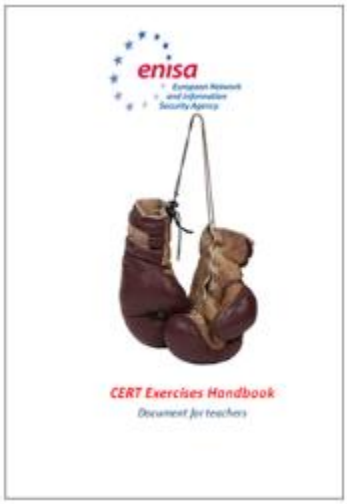
security. In addition, the awareness and perception of Article 14 on Requests to the Agency, was examined following an increase in related work for ENISA over the past years. Article 14 relates to requests for advice and assistance falling within the Agency's objectives and tasks. In practice, requests include support information sharing projects driven by the CERT community, various trainings, assistance in enhancing the cybersecurity capabilities and support to specific projects, for instance honeypots or sensors.

4.2.1 Respondent awareness of related activities

Both the respondents from the n/g CERTs, as well as EU officials displayed a high level of awareness of ENISA capacity building activities in support of CERTs. The majority of the respondent had participated in either trainings or exercises and were well familiar with the materials. Notably, there was a high awareness of training and exercises being delivered in specific areas (e.g. malware analysis or CERT-LEA training). Some of the respondents had also contributed to the development of training materials or even delivered training, such as, for example, as part of the TRANSITs initiative. In contrast to CERT representatives, non-CERT respondents displayed a general level of awareness of ENISA training, but they were less aware of the nature of specific ENISA training courses.

4.2.2 Respondent appreciation of related activities

Overall, the ENISA trainings were viewed very positively, and the respondents were generally satisfied with the types of trainings on offer. Existing trainings were seen as specifically useful for CERTs in the early stages of their lifecycle or for introducing new team members to a CERT environment. However, also non-CERT practitioners, including policy-makers and LEA representatives who had attended ENISA trainings applauded the quality of the courses [27].



Among survey respondents who had attended ENISA trainings, the majority found the ENISA CERT trainings and the related materials relevant and useful. Several respondents praised the newly added technical trainings, which they regarded as being up to date and very useful for CERTs. Also, the TRANSIT I and II trainings[7] received a high level of appreciation. Notably, policy-makers and LEA representatives also applauded the quality of ENISA training courses they had attended.

Across the board the perception is that ENISA has made a significant contribution in relation to the cooperation with and support to national CERTs (for instance, set-up of CERTs and trainings). Indeed, the important role of ENISA events in facilitating trust building between communities and forming a closer network was recognised by many respondents, and this was seen as a particular strength of ENISA's training and workshop events, especially in light of the geographic dispersion of the European CERT community [27].

[7] Parts of the TRANSITS training are based on exercises provided by ENISA. ENISA supports the training through sponsoring and providing tutors when needed and possible.

In relation to ENISA reports, one respondent suggested that ENISA, thanks to the fact that they are able to work with longer time frames (6 months), could pick up more of the topics arising from the CERT community around Europe or even spend time examining and researching new threats more in-depth coming from the more operational CERTs. ENISA has the added value of being able to do this type of research that the CERT community is aware of, but which it is not able to look into due to a lack of time and the nature of their day-to-day work. Similarly, one respondent saw a possibility for ENISA to develop a 'playbook' on major cyber-attacks, which could be used by operational staff who see the issues regularly, but who do not have the time to capture all cases and write them down with recommendations on how to tackle different types of attacks.

This would allow for a categorisation of attacks and a description on the required course of action, including specific tasks, which would make the work more systemic. Another respondent stressed the need to find the right information, for instance tools and databases, when handling security incidents, or having access to technical analysis and recommendations for security incident analysis, as well as identification and threat information sources.

A respondent from the EU institutions noted that while the ENISA reports are good and mostly relevant for EC officials, they are oftentimes directed at the CERT community and not at policy makers. Hence, it would be useful to have an overview of why CERTs matter and what they can do and cannot do. This could be an important awareness raising tool. Moreover, it was suggested that ENISA had more of its publications translated so as to reach an even wider audience.

Among CERT staff and EU officials, knowledge of the possibilities afforded by Article 14 for advice or assistance was generally quite low among both. However, among those aware, and those who had previously requested support under article 14 from ENISA, the respondents reported a high level of appreciation for the support received as it was in line with their expectations.

4.2.3 Perceived weaknesses of related activities

While not a shortcoming of ENISA as such, several CERT respondents underlined that they were often unable to attend ENISA trainings as their team could not afford their absence or because the financial resources necessary for attending training sessions were unavailable. It was suggested that a possible solution to this problem could be for ENISA to offer more online training courses or make accessible pre-recorded training materials in the future.

A few CERT respondents suggested that ENISA training material could be more detailed and that the technical content, which was generally viewed positively, could be evolved and updated. Others noted that the material could be improved through more operational feedback from those using the training material on the frontline.

Concerning future ENISA workshops, some respondents floated the idea of ENISA engaging in more sector orientated training to allow for detailed discussions on specific technical matters among the more advanced CERTs.

However, the same respondents also noted that the offering of more specific technical training courses could come at the expense of approximating n/g CERT capabilities across Europe. Another respondent reported that the training courses were often too short, with the ideal length being 3-4 days [27]. A comment was made that in some areas ENISA's workshops had been weak because they had failed to build upon each other. This implicitly raised the question whether training sessions had to be accessible for newcomers or whether they should be targeted at individuals with prior knowledge in the area explored.

In addition, concerning the CyberEurope exercises, one respondent suggested that the preparation of exercises could be more efficient, with the aim being that exercises could be run at an increased

tempo. Conversely, another respondent noted that one exercise every two years was sufficient because of resource constraints within ENISA and the CERT community [27].

One weakness brought up by one of the interview respondents is the difference in pace between the time it takes ENISA to produce a report in line with the Work Programme versus how fast things are moving in reality. This means, for instance, that tasks identified for the annual Work Programme 2014 will only be implemented by the end of 2015. In the meantime, issues like Heartbleed occur, while ENISA must still fulfil targets that were set two years earlier. This issue was discussed during the validation workshop, and although no obvious solution around the current way of working was identified, it was suggested that the use of requests under Article 14 could be used as a leeway to introduce more current events to the tasks of ENISA.

One question put to the respondents was whether ENISAs activities respond to the needs of the CERTs. The answers were somewhat conflicting, suggesting that there is a need for ENISA to raise awareness about its actual mandate as outlined in the new ENISA basic Regulation (see chapter 3) and the actual tasks it delivers in order for CERT community to better discern between what ENISA could do as opposed to what they should do.

For instance, one respondent expressed the view that it would be better if ENISA focused on fostering cooperation between CERTs instead of doing internal CERT work. This view is contrasted by another respondent suggesting that while strategy work is good, it would also be useful if ENISA increased the support of the operational CERT teams, and helped them to reduce the workload by supporting the work on automation. Additionally, working on reducing legal uncertainty through information exchange emerged as a desirable direction. Similarly, one EU official suggested that, if done gradually, ENISA could move into more operational and technical tasks in the coming years. This would represent a significant shift and a challenge for ENISA as the organisation is perceived as only writing studies.

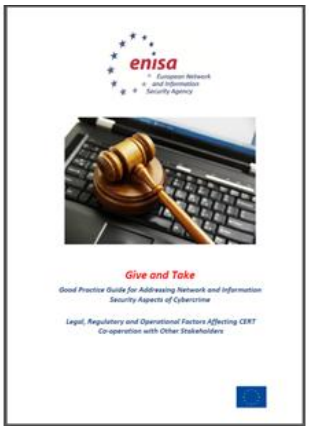
4.3 Support for CERT – LEA Cooperation

2010 was the start of ENISA's support for operational collaboration between the CERTs in the EU Member States and Law Enforcing Agencies (LEA). Since then, various activities have been launched, including stock takings of legal and operational obstacles that prevent collaboration, advice resulting from that, workshops that brought together members of both communities, consultation with members of both communities, etc. Already at the early stages of the operational collaboration, it became clear that the process of trust building, tackle obstacles jointly, discussion and finally working together requires a great deal of time and active, continuous support from ENISA, CERTs and LEAs.

Part of the rationale behind ENISA's involvement is linked to the inherent nature of cybercrime as a global and not a "sectorial" problem, which has sparked calls for cross-border and cross-sector collaboration. In light of this, ENISA's role is to foster cooperation among CERTs, and among CERTs and other stakeholders. Concretely, ENISA's work in this field translates in support for CERT – LEA cooperation.

In addition to joint workshops with select stakeholders on cybercrime, ENISA contributions in this area include the following Good Practice Guides:

- Legal Information Sharing;
- Supporting Fight Against Cybercrime;
- Good practice Guide for Addressing Network and Information Security Aspects of Cybercrime;
- A Good Practice Collection for CERTs on the Directive on attacks against information systems.



4.3.1 Respondent awareness of related activities

In general, there was a high level of awareness about ENISA's activities in supporting CERT cooperation with LEAs. A high-number of respondents had been previously involved in ENISA workshop preparations or had attended LEA-CERT workshops. However, despite the awareness among the interview respondents, several indicated that raising further awareness of the promotion of cooperation between CERTs and LEAs would require considerable effort. Specifically, respondents noted that in some of ENISA's activity areas the outputs failed to reach the right stakeholders at national level, although it was also recognised that ENISA could only exercise limited control over this [27].

Closely linked to the support for the LEAs is the fight against cybercrime, which ENISA is also actively involved in. Among the survey respondents who had taken part in or made use of ENISA's support activities in the fight against cybercrime the majority indicated that they had attended trainings on the subject.

4.3.2 Respondent appreciation of related activities

The main message from the respondents was that ENISA is perceived as doing important pioneering work in advancing the dialogue among CERT and LEA representatives. For instance, one respondent explicitly stated that ENISA got a "phenomenal amount of work" [27] done in terms of strengthening CERT-LEA cooperation, especially in the light of ENISA's limited resources.

Several respondents stressed the importance of ENISA's convening power, in relation to bringing together the LEAs and the CERT communities, as a relatively neutral player to gather people around the table, even when they might have very diverse interests. Appreciation was particularly expressed for the joint LEA-CERT workshops ENISA had organised. Specifically, various respondents suggested that the workshop in The Hague[8] had been a good example for how both sides started to learn about and from each other [27]. The CERT – LEA workshop conducted in Prague[9] also received high levels of appreciation from several respondents.

Another strength, which may facilitate ENISA's attempts to convene key players, was the credibility of the organisation within the EU, and even internationally, as the voice of European CERTs. This was seen as especially important, but perhaps not exploited enough, with regard to the articulation of CERTs' perspective in major policy decisions, such as, for example, with regard to the NIS Directive or the 2013 Data Protection reform package decisions [27].

4.3.3 Perceived weaknesses of related activities

Despite a significant amount of positive feedback, an ambivalent sense of appreciation was expressed with regard to ENISA's CERT cooperation support activities in the domain of CERT-LEA cooperation. Thus, most respondents accepted that this domain was challenging for ENISA because of some complex, deep seated structural reasons, which were neither easily nor swiftly resolved. Indeed, it was felt that there was still a big gap in understanding between the two communities and a level of mistrust driven, according to one respondent, by the differing institutional attachments of LEAs in the different Member States (e.g. attachment to the interior ministry, military, etc.) [27].

Respondents also noted that the existence of entrenched positions, the diametrically opposed working cultures, and complex operational rules inhibited the support ENISA could give to CERT-LEA cooperation. However, as one respondent pointed out, the reasons for levels of attendance at related ENISA events, simply stems from a lack of specialised police personnel. During the validation workshop, one participant argued that cooperation could be facilitated by initial contact and collaboration at higher levels within the organisations involved, which could allow for a trickle-down effect.

Notwithstanding the reservations outlined above, respondents accepted that CERTs and LEAs need to work together and that ENISA is well placed to make that happen. In this respect, it was highlighted that ENISA's good practice guides could benefit from being more sector specific [27]. Moreover, some respondents noted that despite co-operation and liaison agreements between ENISA and the EC3, ENISA could do even more to provide an institutional foundation to the promotion of CERT-LEA cooperation.

Some of the perceived weaknesses related to this activity pillar was ENISA's lacking ability to disseminate information about its work. In the words of one of the respondents: "ENISA has provided great input in the battle against botnets, but their products have not been marketed enough". The same respondent stated that ENISA should focus more on getting their products to the interested parties, as "They have loads of interesting material that has been used by some countries to establish national

[8] 7th CERT Workshop – Part II, October 2012, co-organised with Europol.
[9] 6th CERT Workshop, October 2011, on Addressing NIS aspects of Cyber Crime

CERTs. However, it is not well known". Moreover, it was not seen as enough to simply have a website from which material can be downloaded– there must be direct links to the material so as to attract the users. Finally, one respondent pointed out that most ENISA reports can mainly serve a strategic purpose, whereas it would be interesting to have some more operational information. The Europol "cyberbits" mailing list was put forward as an example which provides concise and actionable information about new phenomena as they occur.

4.4 Summary Table of ENISA Impact - Operational Perspective

Impact on Baseline Capabilities for CERTs		
Respondent awareness	**Respondent appreciation**	**Perceived weaknesses**
1. Baseline capability guides/events are well known & "on the radar screen" 2. There is a difference in awareness between CERTs (high) vs. other operational communities (lower)	1. Good practice guides for start-up CERTs from scratch are good 2. Guides and tools are valuable 3. Reports have a high quality 4. ENISA has a deep community understanding 5. Guides should funcition as tool for "regulating" the CERT community	1. Need to cater to new vs. advanced CERT teams 2. Need for support throughout CERT lifecycle 3. Improved dissemination of materials 4. No "one-size fits all" – tailored to sector 5. Shorter guides/ frequent updated
Impact on Capacity Building for CERTs		
Respondent awareness	**Respondent appreciation**	**Perceived weaknesses**
1. High level of awareness /participation in past events 2. Difference in awareness CERTs (high) vs. other operational communities (lower) 3. Low awareness of Article 14 requests	1. High appreciation for ENISA trainings 2. Significant ENISA contribution to cooperation and support to n/g CERTs (incl. set-up of CERTs and trainings	1. Call for more online courses / 3-4 days trainings 2. More technical updates of materials 3. In-depth research into issues from MS 4. Difference in pace between the time to produce a report in line with the WP vs. the real pace of events
Support for CERT – LEA Cooperation		
Respondent awareness	**Respondent appreciation**	**Perceived weaknesses**
1. High level of awareness of CERT-LEA support 2. For some activity areas the outputs failed to reach the right stakeholders at national level 3. Respondents made use of ENISA's support activities in the fight against cybercrime	1. ENISA is pioneering in advancing the dialogue among CERT and LEA representatives 2. Strong convening power ENISA credible as European voice for CERTs (EU & beyond)	1. Good practice guides could become more sector specific 2. Improved marketing 3. Could provide an institutional foundation to the promotion of CERT-LEA cooperation

5 Respondent 360° Feed-Back

As mentioned in the description of the methodology of this study, a semi-structured approach was employed during the interviews in order to allow for the respondents to freely express their views on ENISA's support to the CERT community. However, much of the respondents feed-back was not directly linked to the ENISA three activity pillars (baseline capabilities, capacity building and support for CERT - LEA cooperation) presented in chapter 4.

Therefore, this chapter serves to capture a number of respondent views (from the interviews and surveys) in order to provide a 360° understanding of the possible future direction of ENISA CERT related support.

5.1 Suggestions for Future ENISA CERT Activities

The open-ended question on what CERT-related areas should ENISA put more focus in the coming five year period sparked a great variation of answers. The feed-back from several respondents stressed a "more of the same" answer, indicating that they primarily want to see ENISA continue doing what it is currently doing.

While this strongly indicates that ENISA is fulfilling its role, several of the answers also pointed to a need for a deepened mandate and a partly broadened scope, including technical tasks. As CERTs around the EU are growing in number and becoming increasingly mature, it is only normal that the requirements of ENISA develop over time.

5.1.1 Improved communication and enhanced information sharing

Several respondent comments highlighted the need for more general CERT relevant information about incidents and threats on the one hand, but also about the role and actual tasks of ENISA on the other, which somehow escapes parts of the CERT community. This leads us to conclude that ENISA needs to review its information channels, the frequency of messages/communication to the community and, possibly, the types of information it communicates.

Reinforced Information Exchange

The need for ENISA to engage more in information sharing about threats and attacks was a recurrent theme coming from several respondents. However, some respondents expressed criticism related to the fact that ENISA is publishing information on its website about incidents and attacks, for instance Heartbleed, with some delay and without regular updates.

The lack of updates made the post obsolete and gave ENISA a bad image as it did not align its advice with that of other authorities in the CERT community. In conclusion, there is support for ENISA alerting and informing the CERT community on attacks and incidents, but it is imperative that the information stays up to date with the developments as they unfold.

Improved Channels of Communication

One respondent from the EU institutions stated that the EU has 28 Member States, all of which should have a CERT. However, for him as a CERT expert, he did not know how he could get in touch with respective national CERT and argued that this is the kind of information he would expect ENISA to provide. This is a striking example of information that ENISA is already providing on its website, but which appears to go unnoticed by some members of the CERT community.

In fact, ENISA does have an interactive map displaying "CERTs by country"[10] on its website, allowing for users to search among EU and EFTA countries and filtering by various types of CERTs ranging from national/governmental, to commercial and academic. This is one case of accessible information, that could benefit from a differently structured website and/or by better dissemination of information, which would be done in relation to CERT trainings, workshops and meetings or in the quarterly reviews.

ENISA as a CERT Community Connector and Facilitator

Several respondents stressed the need for ENISA to continue to play its role as a facilitator for CERT related activities in Europe. This includes stronger cooperation and information sharing between CERTs, as well as with other operational communities which go beyond the "classical CERTs", as well as academia, industry and the commercial environment.

Moreover, ENISA should strengthen the relations with NREN CERTs and commercial CERTs, not only the governmental or national ones. ENISA's role as connector was seen to be achieved through networking events, mainly in relation to its workshops and seminars. Examples of ways of facilitating contact put forward included the use of a functional mail box or by dedicating a page on the ENISA website.

5.1.2 Harmonisation and Common Standards

Accreditation and certification of CERTs

A number of respondents pointed to the fact that while the set-up of CERTs around the EU Member States and the establishment of a full coverage in terms of n/g CERTs was sufficient, the next and equally important step concerns supporting CERTs maturity.

The suggestions in relation to the maturation of CERT teams relate to the harmonisation of baseline requirements with established CERT-related requirements. Accreditation and certification of teams play a crucial role in creating a benchmark across the board. In this respect, ENISA could contribute by establishing a list of reconginsed entities of CERT accreditation and certification.

"We are not so many in the CERT community – we should be able to be better organised. "[1]

Another recurrent theme highlighted the need to develop and use common standards and tools across CERTs. The respondents underlined the increasingly important contributing factors in ensuring maturity of teams and a working CERT infrastructure that need to be addressed by ENISA as well, as described in the section below. Some respondents stated that this is an area where ENISA could play a crucial role.

5.1.3 Compilation of Protection and Detection Methods

In light of a growing fragmentation of incident detection and handling procedures, coupled with a general lack of resources available, several respondents stressed the need for research into protection and detection methods/tools that work everywhere, are affordable to develop (or already existing functionality) and reliable (i.e. no false positives).

This work is important since resources are already scarce and they need to be used wisely, i.e. operational staff need to work on resolving issues as they occur, and not just identify incidents. ENISA is seen as being in a good position to identify and re-use tools from the various Member States. It was suggested that ENISA could oversee the creation of a catalogue, testing and validation of common tools for all MSs, which could be re-used in the global cyber world. As one respondent stated: 'There are so many things you can do, which are not being done in favour of more complex and expensive checklist-

[10] http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

security projects that have little to no effect. One example of effective and easy tools are fake datasets that ring the alarm when being accessed (i.e. honeytables and honeyfiles)'.

In fact, a pilot site for a proposed collection of tools and guidelines of their use intended for incident handling teams has already been created and is available on the ENISA website as a 'Clearinghouse for Incident Handling Tools'[11]. The information on the site was collected to create a repository of information about tools that were actively used and supported by active CERTs.

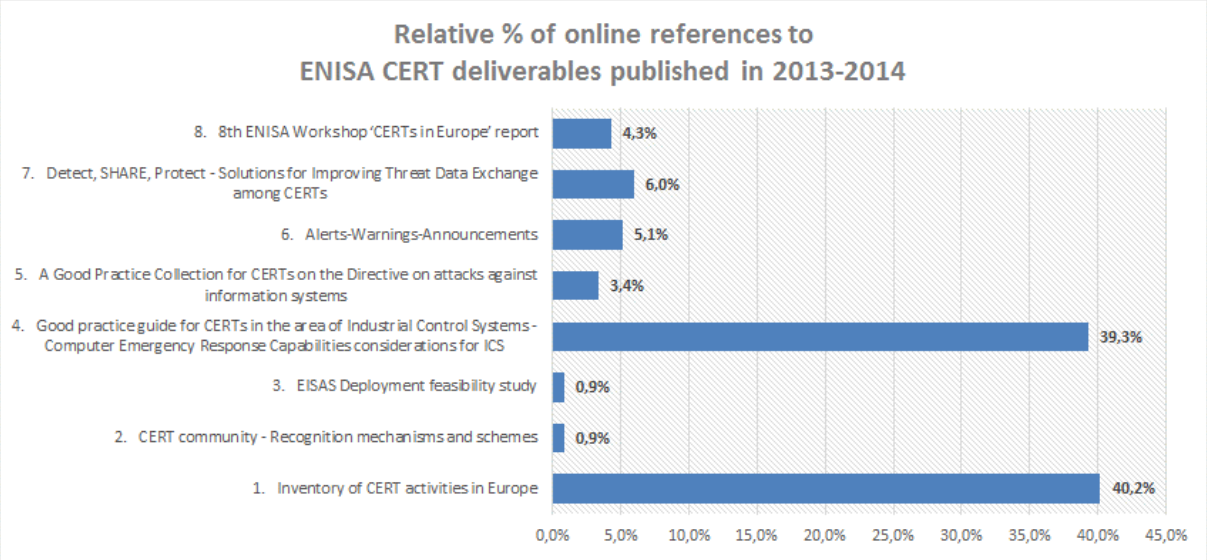
While this is another example of the need for greater awareness-raising about ENISA activities, it also shows that ENISA does not have to re-invent the wheel in terms of new activities. In this case, it would suffice to re-launch the effort.

[11] https://www.enisa.europa.eu/activities/cert/support/chiht

6 Web Impact Analysis

In addition to the qualitative findings, the results from the quantitative web-impact analysis have been included to highlight the online impact of a number of recent ENISA CERT publications.

As mentioned in the methodology chapter, a web impact analysis was performed on a select number of ENISA CERT-related deliverables with a view to get an understanding of the online impact of ENISA's publications. In other words, how wide is the outreach of ENISA's deliverables aside from what is published on its website.



Two of the ENISA CERT-related deliverables are obviously the ones that were referred to (via links included in the web sites) they triggered significantly higher interest from the community and apparently were considered as worthy to be made available on a more permanent basis and to a larger audience of stakeholders.

6.1 Scope

The scope of the web impact analysis focused exclusively on ENISA deliverables published in 2013 and 2014, as presented in the following list:

- Inventory of CERT activities in Europe [29];
- CERT community - Recognition mechanisms and schemes [30];
- EISAS Deployment feasibility study [31];
- Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS [32];
- A Good Practice Collection for CERTs on the Directive on attacks against information systems [15];
- Alerts-Warnings-Announcements [33];
- Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs [10];
- 8th ENISA Workshop 'CERTs in Europe' report [34];

6.2 Results

In terms of results, displayed in the graph above, the search revealed that the top three deliverables, i.e. the ones that are the most referenced to, include:

- Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS;
- Inventory of CERT activities in Europe;
- Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs.

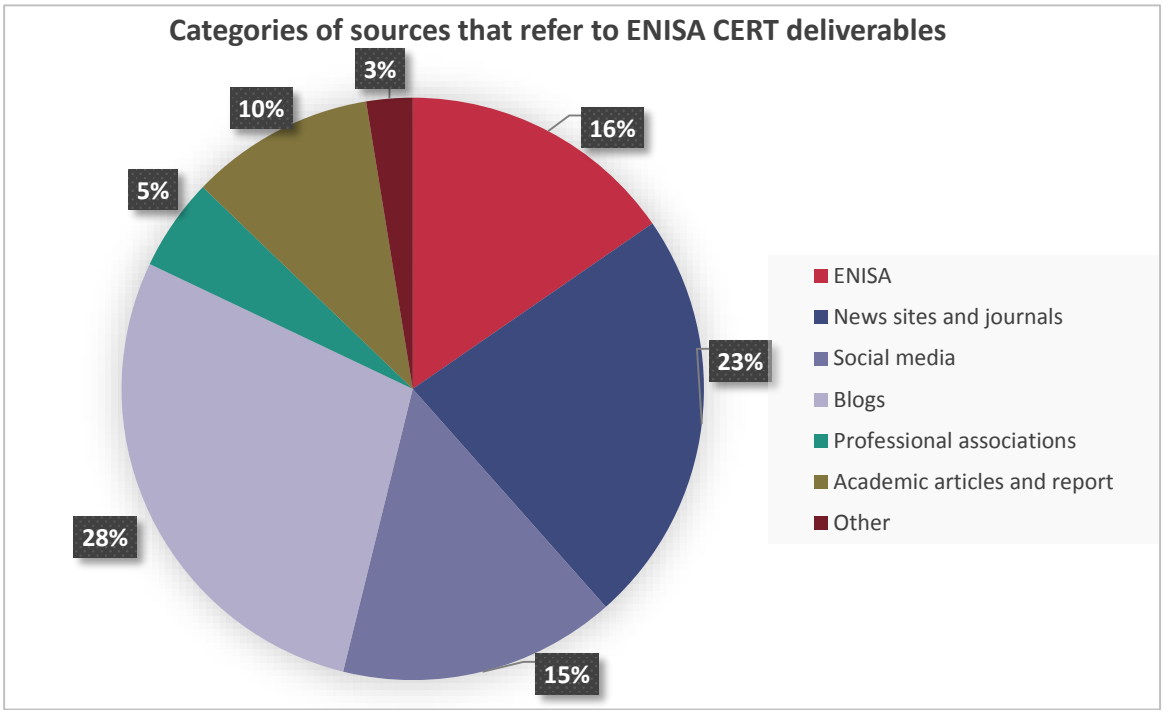
On the other side of the spectrum, the following three deliverables did not appear as referenced at all:

- CERT community - Recognition mechanisms and schemes;
- EISAS Deployment feasibility study;

A possible explanation for the lack of online references for these three deliverables may be due to the fact that for none of them there is a mention or link to the corresponding deliverable from one level up in the hierarchy of the ENISA website. In other words, as opposed to these low-scoring deliverables, the ones that had been more frequently referenced to were also mentioned more frequently on the ENISA website.

Another part of the results of the web impact analysis relates to the categories of sources the ENISA deliverables were references on. From the search conducted, it can be concluded that the top three sources of categories (not taking into account the ENISA website) that reference the most to ENISA CERT related deliverables include blogs; news sites and journals; and professional associations.

The results of the analysis using the *allintext* Google search operator have been grouped in the above mentioned categories as visible in the graph below.



The graph above indicates that ENISA CERT deliverables published in 2013 – 2014 are more popular on the social media, blogs and news/journal sites than in the academic or professional associations sites.

7 Link with 2009 Survey Results for ENISA CERT-related Activities and Deliverables

In this chapter, we highlight the most relevant aspects that are common to the survey made in 2009. The intention is to summarise relevant differences and trends concerning ENISA CERT related activities and deliverables.

7.1 Summary of the main results of the 2009 report

A number of attention points were identified in order to be considered by ENISA and specific recommendations for improvement were captured from the respondents to the survey. The qualitative analysis of these revealed a large number of very constructive suggestions, and only a limited number of unsatisfied stakeholders.

The participation from the governments of the Member States and from the national regulators was strong. The poor level of participation from the ENISA Management Board Members and from the ENISA Permanent Stakeholder Group may be eventually explained by the fact these stakeholders have additional channels established for providing ENISA with direct input on the activity of the Agency and on the deliverables issued.

The ENISA website, the ENISA Quarterly Review and the ENISA reports are the most familiar and effective ENISA communication channels towards the stakeholders. The ENISA events and the NIS brokerage co-operation initiatives are less known.

The ENISA website is clearly the preferred channel of the stakeholders both in terms of familiarity with it and in terms of main source of information. Most of the respondents agree that ENISA website is useful. However, more interactive media should be used that can be directly accessible via the ENISA website: RSS, podcasts, blogs, etc.

The ENISA Quarterly Review is well written, objective and accurate. Stakeholders would recommend the ENISA Quarterly Review to others. However, improvements are required in making this deliverable less theoretical and richer in statistics, trends, facts and other hard data on NIS issues of interest.

In general, the overall feed-back on individual ENISA reports is very positive all dimensions analysed: Usefulness and value provided by the report; Content aspects; Achievement of the individual report's objectives. The only dimension where there was a relatively higher need for focus from ENISA is the one related to the comprehensiveness of the reports.

There is a need for better and more structured communication and dialogue with all groups of NIS stakeholders. According to the ENISA Management Board members, they do not have sufficient means to provide ENISA with sufficient questions/feedback.

The ENISA participation in events is considered as adequate and useful. In some cases ENISA presentations at events have triggered awareness campaigns, creation of national CERTS, changes in strategies, policies and procedures. However, there is a need for ENISA to provide more actionable suggestions and guidance during events, in order to support practical implementations.

ENISA NIS brokerage co-operation initiatives are less known by the stakeholders. The most known was the initiative on establishing of a new Gov-CERT in another Member State. The overall interest of stakeholders in participating in ENISA NIS Good Practice Brokerage cooperation initiatives is relatively low.

7.2 Links with the 2014 Research Results

While the 2014 study focuses specifically on ENISA support to CERTs and related activities, the 2009 study covered the ENISA deliverables produced between October 2007 to the end of 2008, including deliverables from various ENISA departments.

The first objective of the 2009 study was to assess the impact of ENISA's deliverables with respect to dissemination and practical use in the target groups. This can be linked to the second objective of this study of performing an impact analysis of ENISA's achievements with regard to CERTs and other operational communities.

The second objective of the 2009 study was to assess the quality of the width and depth of the achieved dissemination which in this study is encompassed in the survey and interview questions.

The third objective was to compare the findings of the new survey to the previous ones in order to identify the progress being made by ENISA. This study does compare findings to the previous study. In addition, it uses the 2009 study as a basis for assessing the impact of ENISA's achievements with regard to CERTs and other operational communities.

The results achieved by the 2009 survey provide a basis for further assessing the impact of ENISA's output and for directing future activities to enhance the focus of the ongoing work of the Agency to its strategic objectives. The results of this 2014 study generally correspond to those from the 2009 survey especially concerning the overall feed-back on individual ENISA reports which is positive.

8 Conclusions and Draft Roadmap Towards 2020

This Chapter concludes the impact assessment of ENISA CERT support activities by proposing an indicative roadmap for future activities of ENISA on the basis of the findings presented in Chapters 3-5, as well as the validation of the Expert Group.

8.1 Overall Conclusions

This report represents the outcome of an impact assessment performed by Deloitte of ENISA's support to Computer Emergency Response Teams (CERTs) for the period 2005 until 2014. The impact assessment has served as a basis for the proposed roadmap to 2020.

The key objectives of the study have been to:

- Take stock of ENISA achievements in relation to European CERTs, and in light of relevant policy documents;
- Perform an impact analysis of ENISA's achievements with regard to CERTs and other operational communities;
- Provide a roadmap for the period leading up to 2020 based on the results of the impact analysis.

The study of ENISAs CERT support has been conducted following a dual perspective:

- Policy and regulatory;
- Operational.

Chapter 3 covered the legislative and regulatory perspective, by examining key policy and strategy documents, such as the DAE, the Cybersecurity Strategy of the EU, the ENISA Regulation and the ENISA annual Work Programmes 2013 – 2014, as well as the proposed NIS Directive. Based on the desk review and respondent input[12], the study team concludes that ENISA's role and impact in this domain is recognised, as reflected in the increasing scope and authority extended over time to the Agency.

The operational perspective, presented in chapter 4 followed the logic of the ENISA activity pillars; baseline capabilities for CERTs, capacity support for CERTs and support for CERT- LEA cooperation, and was based on the results from the interviews and the surveys. The awareness of ENISA's CERT support actions is high in the constituency, and there was overall a positive view of the work ENISA was performing to support CERTs. As for the baseline capabilities, there was an expressed need to keep the baseline capabilities more separate from the capacity building activities as the former should cater to the needs of CERT teams of varied levels of maturity.

There was high level of awareness among the respondents of ENISA's capacity building activities (primarily trainings, workshops, exercises and dissemination of good practices). However, the findings show that awareness is higher among representatives of n/g CERTs than among other CERT communities. Main findings related to the trainings also include a need for a clearer message in terms of the level of prior knowledge needed to participate in different trainings, as well as a need for more online training resources to be accessible via the ENISA website.

When it came to the ENISA reports, there is need for more technical topics on the one hand, and more policy-related related reports on the other hand. The latter could serve to make the case of the ENISA *raison d'etre* to policy and decision-makers. It was also suggested that ENISA picks up topics and current trends or threats from the EU Member States to carry out in depth research on them and it presents results in a way that it can be translated to several languages.

[12] Proposed actions are included in the roadmap.

ENISA's support for CERT-LEA cooperation, although hampered by the differences in cultures between organisations, was hailed in light of ENISA's ability to attract the right players and for advancing the dialogue between the CERTs and the LEAs. The credibility of ENISA as the voice of European CERTs within the EU and beyond was undisputed.

Despite this, some areas were still considered as requiring more attention. For instance, the ENISA reports thus far serve more a strategic than an operational purpose. This included more specific good practice guides to serve the stakeholders, as well as more operational information. Greater awareness raising of the guides and reports was also stressed as necessary to reach out to the LEAs, as well as to other operational communities.

Charter 5 captured a wider range of respondent views**,** providing additional suggestions on possible areas in which ENISA could deepen and/or expand its support to the CERT community. The key points raised focused on ENISA as a CERT community connector and facilitator, within and beyond the traditional CERT stakeholders. The need to improve ENISA's channels of information was another strong point, requesting ENISA to better disseminate information via its website, or in relation to trainings and workshops, as well as alerting the CERT community and other operational communities on attacks and incident. There was also a call for greater harmonisation and common standards coming out to the respondent feed-back.

8.2 The Way Ahead: Roadmap for ENISA CERT Support

The proposed high-level road map 2020 presented below provides an overview of possible areas of priority on the basis of Chapters 3 - 5. Of course, the roadmap can only be executed if resources within the ENISA CERT Support team allow it. This roadmap must be taken as a way to go forward, and not as a commitment on ENISA's part to execute it as-is, after prioritisation and resources allocation.

8.3 High-Level Roadmap to 2020

Legislative & Regulatory: Proposed Actions	Complexity	Dependencies	Resources	Timeline
Act as a representative voice for CERTs in the European policy context	Medium	Collection of perspectives from CERT community on relevant policy documents	High	Medium – long term
Cybersecurity Strategy: • Assist in the creation of cross-border operational procedures and crisis management processes; together with technical guidelines and recommendations for national cyber resilience capabilities. • Develop and promote models of cooperation which have good balance between declared level of response or provided (voluntary) services; mandatory obligations (e.g. NIS directive, telecom package); Incentives for cooperation in the form of tangible benefits;	Medium	Acceptance and support from CERTs and relevant stakeholders	High	Medium – long term
	Medium	Acceptance and support from CERTs and relevant stakeholders	High	Medium – long term
NIS Directive: • Create guidance for CERTs to locally comply with provisions of NIS Directive • Enable national CERTS to support other CERTs in the different industries such as finance, and CIIP by promoting the increase of support from the ministry level for which ENISA could assist in raising awareness on this strategic level.	High	Adoption of the proposed NIS Directive	High	Medium – long term
	Medium	Adoption of the proposed NIS Directive	High	Medium – long term

Operational - Baseline Capabilities for CERTs: Proposed Actions	Complexity	Dependencies	Resources	Timeline
Continued support for new CERTs - clear focus on "new team support": • Regular updates of CERT baseline capability materials • Greater focus on technical updates, checklists, summaries	Medium	Anticipation of future change with regard to baseline capability building	Medium	Medium – long term
Reinforced Information Exchange and Connector Role: • Improved communication and enhanced information sharing • Website – mailing lists – networking	Medium	Up to date information and feedback from stakeholders	Low	Short – medium term
Raise awareness and take-up of ENISA materials (baseline capability) by advertising them more widely, and measuring impact in the CERT community and other operational communities	Low	Up to date information and feedback from stakeholders	Medium	Medium – long term

Operational - Capacity building for CERTs: Proposed Actions	Complexity	Dependencies	Resources	Timeline
Continued support for mature CERTs and regularly update CERT baseline capability material with a clearer focus on "advanced team support" for mature CERTs • Regular updates of CERT capacity building material • Greater focus on technical updates, checklists, summaries	High	Acceptance and support from CERTs	Medium	Medium – long term
Reinforced Information Exchange and Connector Role: • Improved communication and enhanced information sharing • Website – mailing lists – networking	Medium	Up to date information and feedback from stakeholders	Low	Short – medium term
Clearer focus on operational vs strategic reports: • More technical reports for practitioners • Policy-related reports for decision makers	Medium	Up to date information and feedback from stakeholders	Medium	Short – medium term
Raise awareness and take-up of ENISA materials (capacity building) by advertising them more widely, and measuring impact in the CERT community and other operational communities	High	Feedback from stakeholders	Medium	Short – medium term

Operational actions: Support for CERT-LEA cooperation: Proposed Actions	Complexity	Dependencies	Resources	Timeline
Facilitate more joint CERT-LEA events and training	Medium	Development of even more training products Stronger CERT-LEA cooperation	Low	Short – medium term
Enhanced support to the fight against cybercrime	Medium	Acceptance and support from CERTs	Medium	Short – long term
Raise awareness and take-up of ENISA materials (CERT-LEA) by advertising/disseminating them more widely, and measuring impact: • CERT community • Other operational communities (LEAs etc.)	High	Feedback from stakeholders	Medium	Short – medium term

360 Feed-back: Proposed Actions	Complexity	Dependencies	Resources	Timeline
Awareness raising: • Key publications • Trainings • Events • Clarification of ENISA role vis-a vis CERT community	Medium	Up to date information and feedback from stakeholders	Low	Short – medium term
Establish a list of reconginsed entities that could be valid accrediators of CERTs accreditation and certification	Low	Acceptance and support from CERTs	Low	Short – medium term
Identification and promotion of common standards for CERT community and other operational communities	Medium	Feedback and support from CERTs/other operational communities	Medium	Medium –long term
Compilation of protection and detection methods: • Continue past efforts - regular updates of "Clearinghouse for Incident Handling Tools" on the ENISA website	High	Feedback and support from CERTs/other operational communities	Low	Medium –long term

Annex – 1 List of Interview Questions

	Question
1.	To what extent do you agree with the following statement? "ENISA has successfully implemented the CERT relate activities set out in the Annual Work Programmes, in the past five (5) years."
2.	To what extent you do consider that ENISA was successful in its mission of supporting the national / governmental CERTs at both the operational and policy level?
3.	To what extent are ENISA CERT activities important in supporting the Cybersecurity Strategy of the European Union, in particular the goals related to co-ordination between NIS competent authorities, CERTs, law enforcement and defence?
4.	To what extent do you agree with the following statement? "ENISA has been successful in disseminating good practices to relevant CERT stakeholders."
5.	To what extent do you agree with the following statement? "ENISA has been successful in achieving the objectives outlined in the ENISA Regulation in relation to support to CERTs in EU Member States."
6.	How well do ENISA CERT activities support the implementation of applicable/relevant EU or national regulations?
7.	To what extent do you agree with the following statement? "ENISA has achieved its objective to develop relationships and enhance CERT-related cooperation with EU institutions and bodies."
8.	To what extent do you agree with the following statement? "ENISA has made a significant contribution in relation to the cooperation with and support to national CERTs (for instance, set-up of CERTs and trainings)."
9.	Concerning the current focus areas and activities of ENISA, in the area of CERTs and operational communities, what could be additional focus areas and activities to be further considered by ENISA in line with the Cybersecurity Strategy of the EU, and/or beyond for coming five (5) years?
10.	To what extent do you agree with the following statement? "ENISA deliverables address the needs expressed by the national / governmental CERTs in a satisfactory way."
11.	To what extent do you agree with the following statement? "ENISA's CERT related support and activities evolve in line with the needs and priorities of the ENISA CERT community."
12.	To what extent do you agree with the following statement? "ENISA has made a significant contribution in relation to the cooperation with and support to national and governmental CERTs (for instance, set-up of CERTs and trainings)."
13.	To what extent do you agree with the following statement? "Sufficient means and channels are available to the CERT community in order to provide ENISA with feedback, suggestions and questions on its CERT related activities."
14.	What additional CERT- focused areas and activities would you recommend to ENISA, in line with the Cybersecurity Strategy of the EU and/or beyond for coming 5 years?
15.	What is your opinion concerning the current strategic objectives of ENISA that are applicable to CERT area? Do they respond to the needs of your organisation? Are they sufficiently relevant?
16.	What ENISA communication channels are you the most familiar with? Which of them do you find the most useful with regards to the CERT specific activities?
17.	Has the CERT you work for ever made a request for ENISA support under the so-called Article 14?

Question
18. If yes, how successful was ENISA in providing support in line with your expectations under Article 14?
19. Did you recently attend an ENISA CERT-related event (e.g. workshops, conferences)?
20. To what extent do you agree with the following statement? "The topics and presentations at ENISA's CERT related events are relevant and useful to the CERT professionals."
21. Did you recently attend an ENISA CERT-related training?
22. To what extent do you agree with the following statement? "ENISA CERT trainings and the related materials are relevant and useful to the CERT professionals."
23. To what extent do you agree with the following statement? "ENISA CERT-related reports and publications are relevant and useful."
24. Would you recommend ENISA's CERT-related reports and publications to others?
25. To what extent do you agree with the following statement? "The ENISA CERT reports are well written & structured."
26. To what extent do you agree with the following statement? "The ENISA CERT reports meet their objectives."
27. To what extent do you agree with the following statement? "The ENISA CERT reports are sufficiently comprehensive (relevant facts and accurate conclusions)."
28. Are you aware of ENISA's support to CERTs in the fight against cybercrime?
29. Has the CERT you work for taken part in or made use of ENISA's support activities in the fight against cybercrime?
30. To what extent do you agree with the following statement? "ENISA's support to CERTs in the fight against cybercrime has facilitated collaboration with other CERTs and/or with law enforcement agencies."
31. To what extent do you agree with the following statement? "ENISA deliverables tackle the needs expressed by European CERTs in a satisfactory way."
32. To what extent do you agree with the following statement? "ENISA deliverables generally evolve in line with the needs and priorities at the level of the CERTs serving constituency in the EU Member States."
33. What is your perspective on ENISA's role as a facilitator and/or sponsor in relation to CERT activities and what direction do you think it should take for the next five (5) years?
34. In what CERT-related areas should ENISA put more focus, in the coming period?
35. Are you aware of or do you monitor ENISA's CERT activities, such as trainings, workshops and support for CERT set-up, etc.?
36. What ENISA communication channels are you the most familiar with? Check all that apply.
37. In what ways do ENISA activities apply to or do influence the activity of your CERT?
38. Do you effectively make use of ENISA CERT related reports or other materials in the current activity of your CERT?
39. Did you or your CERT colleagues have the opportunity to attend any ENISA CERT related events (such as trainings and workshops)?
40. If yes, to what extent to you agree with the following statement? "ENISA CERT related events are relevant and useful for the activity of my CERT?"

Question
41. Should ENISA take on a more active role in supporting the CERT community outside of the European Union?
42. To what extent do you agree with the following statement? "ENISA has been successful in disseminating good practices to relevant CERT stakeholders among the European institutions."
43. To what extent do you agree with the following statement? "In terms of active support to capacity building for CERTs, ENISA's trainings to technical staff from EU institutions are relevant and useful."
44. To what extent do you agree with the following statement? In terms of cooperation with European institutions, ENISA has achieved its objective to develop and enhance these relationships.
45. What ENISA communication channels are you the most familiar with? Which of them do you find the most useful with regards to the CERT specific activities within the European institutions?
46. To what extent do you agree with the following statement? "ENISA is a primary source of information for my CERT related activities/tasks."
47. Has the EU institution you work for ever made a request for ENISA support under the so-called Article 14?
48. To what extent do you agree with the following statement? "ENISA CERT-related reports and publications are relevant and useful to the professionals in the European institutions."
49. To what extent do you agree with the following statement? "ENISA's CERT related activities address in a satisfactory way the needs of my organisation – as they relate to CERT area."
50. To what extent do you agree with the following statement? "ENISA's CERT related support and activities evolve in line with the needs and priorities of my organisation."
51. To what extent do you agree with the following statement? "Sufficient means and channels are available to the CERT community in order to provide ENISA with feedback, suggestions and questions on its CERT related activities." Did you recently attend an ENISA CERT-related event (e.g. workshops, conferences)?
52. In what ways do ENISA CERT activities apply to your organisation / business?
53. To what extent do you agree with the following statement? "ENISA should collaborate more with academia on supporting CERT developments."
54. To what extent do you agree with the following statement? "ENISA should collaborate more with NIS or cybersecurity professional organisations on supporting the latest CERT developments."
55. How are you using ENISA reports and material related to supporting the CERTs?
56. How are you involved in ENISA activities and events in the domain of supporting CERTs?

Annex – 2 Expert Group Members

Expert	Organisation
Lino Santos	CERT.PT/FCCN (Portugal)
Shin Adachi	Nippon Telegraph and Telephone Company (Japan)
Robert Jonsson	MSB/CERT-SE (Sweden)
Andrew Cormack	Janet

Annex – 3 Glossary

Term	Description
CEPOL	European Police College
CERT	Computer Emergency Response Team
CSIRT	Computer Security and Incident Response Team
DAE	Digital Agenda for Europe
EC3	European Cybercrime Centre
EDA	European Defence Agency
EEA	European Economic Area
EEAS	European External Action Service
ENISA	European Union Agency for Network and Information Security
EP3R	European Public Private Partnership for Resilience
FIRST	Forum of Incident Response and Security Team
ICS	Industrial Control Systems
ICT	Information and Communication Technology
JRC	Joint Research Centre
LEA	Law Enforcement Agency
MS	Member State
N/G CERTs	National/Governmental CERTs
NIS	Network and Information Security
NLO	National Liaison Officers
SSL	Secure Sockets Layer
TERENA	Trans-European Research and Education Networking Association
WP	Work Package
WS	Work Stream

Annex – 4 Bibliography

[1] European Commission, "EUROPE 2020 - A European strategy for smart, sustainable and inclusive growth," 3 March 2010. [Online]. Available: http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf.

[2] European Commission, "COM(2010)245 final - A Digital Agenda for Europe," 19 May 2010. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN.

[3] The European Parliament and the Council of the European Union, "Regulation (EC) No 1007/2008 of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security (Text with EEA relevance)," 24 September 2008. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R1007&from=EN.

[4] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final," 07 February 2013. [Online]. Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667.

[5] European Commission, "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (NIS Directive) - COM(2013) 48 final," 07 February 2013. [Online]. Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666.

[6] The European Parliament and of the Council, "Regulation (EU) No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004," Official Journal of the European Union, 21 May 2013. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN.

[7] H. Bronk, M. Hakkaja and M. Thorbruegge, "A basic collection of good practices for running a CSIRT," ENISA, 22 December 2007. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/guide2/files/a-collection-of-good-practice-for-cert-quality-assurance.

[8] ENISA, "Baseline Capabilities of National / Governmental CERTs - Operational Aspects," 2009.

[9] ENISA, " Clearinghouse for Incident Handling Tools," European Union Agency for Network and Information Security (ENISA), 2005-2014. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/chiht. [Accessed 2014].

[10] ENISA, "Detect, SHARE, Protect. Solutions for Improving Threat Data Exchange among CERTs," ENISA, 2013.

[11] ENISA new good practice guide for CERTs - Issuing alerts, warnings and announcements , "ENISA," The European Union Agency for Network and Information Security (ENISA, 2013. [Online]. Available: http://www.enisa.europa.eu/media/news-items/enisa-new-good-practice-guide-for-certs-issuing-alerts-warnings-and-announcements. [Accessed 2014].

[12] ENISA, "Good Practice Guide for Incident Management," The European Network and Information Security Agency .

[13] ENISA, "A flair for sharing - encouraging information exchange between CERTs," the European Union Agency for Network and Information Security (ENISA) , 2011.

[14] ENISA, "Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime," Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime , 2012.

[15] ENISA, " A Good Practice Collection for CERTs on the Directive on attacks against information systems," the European Union Agency for Network and Information Security (ENISA), 2013.

[16] ENISA, "ENISA CERT workshops," [Online]. Available: https://www.enisa.europa.eu/activities/cert/events/past-events.

[17] "2014 Honeynet Project Workshop," The European Union Agency for Network and Information Security (ENISA), 2014. [Online]. Available: https://www.enisa.europa.eu/activities/cert/events/honeynet-project-workshop. [Accessed 2014].

[18] "European FI-ISAC," [Online]. Available: http://www.cpni.nl/informatieknooppunt/internationaal/european-fi-isac.

[19] TERENA, "TF-CSIRT," [Online]. Available: www.terena.org/activities/tf-csirt/.

[20] FIRST, "Forum of Incident Response and Security Teams," [Online]. Available: http://www.first.org/about.

[21] "TRANSITS training," The European Union Agency for Network and Information Security (ENISA), [Online]. Available: https://www.enisa.europa.eu/activities/cert/events/transits-training. [Accessed 2014].

[22] ENISA, "Work Programme 2013," 27 November 2012. [Online]. Available: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013.

[23] ENISA, "Work Programme 2014," 29 November 2013. [Online]. Available: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014.

[24] The European Parliament and the Council , "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 24 October 1995. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN.

[25] The European Parliament and the Council , "Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data," 18 December 2000. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001R0045&from=EN.

[26] "Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı," Şubat, 2014.

[27] ENISA, RAND Europe, "A Study into ENISA's CERT Support Activities - Taking Stock of Contemporary Activities and their Effectiveness and Proposing a Roadmap for Future ENISA CERT Support," 2014.

[28] ENISA, "ENISA Work Programme 2013," [Online]. Available: https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2013.

[29] ENISA, "ENISA – CERT Inventory: Inventory of CERT teams and activites in Europe," 06 2014. [Online]. Available: https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe.

[30] ENISA, "CERT community: Recognition mechanisms and schemes," November 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/cert-community-recognition-mechanisms-and-schemes.

[31] "EISAS – European Information Sharing and Alerting System: Deployment Feasibility Study," December 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/other-work/eisas_folder/eisas-deployment-feasibility-study.

[32] ENISA, "Good practice guide for CERTs in the area of Industrial Control Systems: Computer Emergency Response Capabilities considerations for ICS," October 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems.

[33] ENISA, "Alerts, Warnings and Announcements: Best Practices Guide," November 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/awa.

[34] ENISA, "8th ENISA Workshop 'CERTs in Europe': Part I – Technical Hands-on Workshop ; Part II – ENISA/EC3 Workshop," 18 November 2013. [Online]. Available: http://www.enisa.europa.eu/activities/cert/support/files/8th-enisa-workshop-certs-in-europe-report.

[35] ENISA, "Roadmap for European Cyber Security Month activities," November 2013. [Online]. Available: http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign/2013.

[36] European Parliament, "Legislative resolution on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))," 13 March 2014. [Online]. Available: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//EN.

[37] ENISA, "A flair for sharing - encouraging information exchange between CERTs," 2011.

[38] ENISA, "Incentives and Challenges on Information Sharing," 2010. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing.

[39] ENISA, RAND Europe, "Incentives and Challenges for Information Sharing in the Context of Network," 08 September 2010. [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing/at_download/fullReport.

[40] ENISA, "A flair for sharing - encouraging information exchange between CERTs," 16 December 2011. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing/legal-information-sharing-1/at_download/fullReport.

[41] The European Parliament and the Council of the European Union, "Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA," 10 March 2004. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0460&from=EN.

[42] H. Bronk, M. Thorbruegge and M. Hakkaja, "CSIRT Setting up Guide - A step-by-step approach on how to set up a CSIRT," 22 December 2006. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide.

[43] European Commission, "Network and Information Security: Proposal for A European Policy Approach," 2001 .

[44] European Commission, ""Impact Assessment - SWD(2013)32 final - 7/2/2013"," 07 February 2013. [Online]. Available: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1669.

[45] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe," 2010.

[46] ENISA, "Clearinghouse for Incident Handling Tools," The European Union Agency for Network and Information Security (ENISA) , 2005-2014. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/chiht. [Accessed 2014].

[47] The Academy for Leadership in International Affairs, "Chatham House Rule," [Online]. Available: http://www.chathamhouse.org/about/chatham-house-rule.

[48] ENISA, "The Directive on attacks against information systems: A Good Practice Collection for CERTs on the Directive on attacks against information systems," November 2013. [Online]. Available: https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems.

[49] ENISA, "A Study into ENISA's CERT Support Activities - Taking Stock of Contemporary Activities and their Effectiveness and Proposing a Roadmap for Future ENISA CERT Support," 2014.

Catalogue Number TP-04-14-910-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

doi: 10.2824/34500

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu