COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

EN   EN

Study on the Evaluation of the European Union Agency for Network and Information Security

Final Report
A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

Digital
Single
Market

This study was carried out for the European Commission by

RAMBØLL

Karin Attström, Vanessa Ludden, Franziska Lessmann
Ramboll

CARSA

Pär Weström, Johannes Conrads
Carsa
Carretera de Asúa, 6
48930 Getxo
Vizcaya – Spain
http://www.carsa.es

With contributions from Helena Farrand Carrapico, Aston University; Andrej Savin, Copenhagen Business School; Cristina de la Maza, RedBorder

Internal identification

Contract number: No 30-CE-0815229/00-33 implementing Framework contract No 30-CE-0677656/00-00

SMART number 2016/0077

CONTENTS

FIGURES

TABLES

APPENDICES

Appendix 1
Evaluation Question matrix

Appendix 2
Bibliography

Appendix 3
Survey questionnaires

Appendix 4
Positioning exercise

Appendix 5
Comprehensive SWOT table

LIST OF ACRONYMS

Acronyms	
ANSSI	National Cybersecurity Agency
BEREC	Body of European Regulators for Electronic
BSI	German Federal Office for Information Security
CA	Contract agent
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Teams
CII	Critical information infrastructure
CIIP	Critical Information Infrastructure Protection
COD	Core Operations Department
cPPP	contractual public-private partnership
CSIRT	Computer Security Incident Response Teams
DAE	Digital Agenda for Europe
DG CNECT	DG Communications Networks, Content and Technology
DG DIGIT	DG for Informatics
DG JRC	Commission Joint Research Centre
EC3	European Cybercrime Centre
EDPS	European Data Protection Supervisor
EFCA	European Fisheries Control Agency
eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	European Union Agency for Network and Information Security
EQ	Evaluation question
ETSI	European Telecommunications Standards Institute
FIRST	Forum of Incident Response and Security Teams
FRA	European Union Agency for Fundamental Rights
FTE	Full-time equivalent
ICT	Information and communication technology
INCIBE	Spanish National Institute for Cybersecurity
IoT	Internet of Things
KII	Key impact indicator
KPI	Key performance indicator
MOOC	Massive Open Online Courses
NATO	North Atlantic Treaty Organisation
NCSC	Netherlands National Cyber Security Centre
NIS	Network and Information Security
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
NIST	US National Institute of Standards and Technology
NLO	Network of Liaison Officers
OASIS	Organisation for the Advancement of Structured Information Standards
PSG	Permanent Stakeholders' Group
QMS	Quality Management System
SESIAD	State for the Information Society and Digital Agenda
SMEs	Small and medium enterprises
SNE	Seconded national expert
SWOT	Strengths, weaknesses, opportunities and threats
TA	Temporary agent
UN/ITU	United Nations' International Telecommunication Unit

ABSTRACT

The European Union Agency for Network and Information Security (ENISA) was established in 2004. The Agency provides advice and recommendations, data analysis, and supports awareness raising and cooperation by the EU bodies and Member States in the field of cybersecurity. ENISA uses its expertise to improve cooperation between Member States, and between actors from the public and private sectors, as well as to support capacity building.

The present study involves the evaluation of ENISA over the 2013-2016 period, assessing the Agency's performance, governance and organisational structure, and positioning with respect to other EU and national bodies. It assesses ENISA's strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It also provides options to modify the mandate of the Agency to better respond to new, emerging needs and assesses their financial implications.

The findings of the evaluation study show that ENISA has made some important achievements towards increasing NIS in the EU. However, a fragmented approach to cybersecurity across the EU and issues internal to the Agency, including limited financial resources, hinder ENISA's ability to respond to the ever growing needs of stakeholders in a context of technological developments and evolving cybersecurity threats.

EXECUTIVE SUMMARY

This is the executive summary to the "Study on the Evaluation of the European Union Agency for Network and Information Security (ENISA)".

Objectives

ENISA is the EU agency for network and information security. It was established in 2004 by Regulation (EC) No 460/2004. Since then, ENISA's mandate has been reviewed once and the Agency's mandate has been extended several times. The latest changes were implemented with Regulation (EU) No 526/2013 (hereafter "the Regulation"). Article 32 (1) of the Regulation requires the Commission to "commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency ad its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification".

The study involves the evaluation of ENISA over the 2013-2016 period, assessing the Agency's performance, governance and organisation structure, and positioning with respect to other EU and national bodies. Furthermore, the study assesses ENISA's strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It provides options to modify the mandate of the Agency to better respond to the new needs and assesses their financial implications.

Methodological approach

The evaluation study aims to assess the relevance, effectiveness, efficiency, coherence and complementarity, and EU added value of ENISA. It contains responses to 46 evaluation questions based on the European Commission's Roadmap for the evaluation of ENISA[1]. The evaluation conclusions are drawn from both primary and secondary data collection and analytical tasks which feed into the development of the answers to the evaluation questions. The evaluation involved extensive data collection, including the consultation of various stakeholders groups (such as ENISA staff and management, ENISA's Management Board, national Computer Emergency Response Teams and Computer Security Incident Response Teams (CERTs/CSIRTs), EU institutions, private stakeholders). Primary data was collected through different tools: in-depth interviews, two surveys, an open public consultation and a workshop. The evaluation is underpinned by an evaluation matrix, which links the evaluation questions to the data sources, indicators and analytical strategies that were used to answer them, thus making it clear how the conclusions have been reached.

The evaluation was carried out between November 2016 and July 2017 by Ramboll Management Consulting and CARSA, and involved three external experts covering the policy, legal and technical aspects of cybersecurity.

Findings and conclusions

An assessment of ENISA's performance, governance and operational structure and positioning for the period 2013-2016 according to the evaluation criteria is presented in the following table. The key findings that have led to this assessment are presented below.

Table 1: Assessment of ENISA against the evaluation criteria

Evaluation criterion	Overall assessment
Relevance	Achieved to a large extent
Effectiveness	Partially achieved
Efficiency	Achieved to a large extent
Coherence	Partially achieved
EU-added value	Partially achieved

---

[1] European Commission (2016): Evaluation Roadmap – Evaluation of the European Union Agency for Network and Information Security (ENISA)

Relevance: In the context of technological developments and evolving threats, there is a significant need for increased network and information security (NIS) in the EU. The recent additions to the legislative framework, such as the NIS Directive[2] underline this. Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. Considering this context, the objectives set out in ENISA's mandate proved to be relevant over the period under evaluation and continue to be of high relevance today.

While the mandate defines the Agency's objectives in broad terms, leaving room for ENISA's Management Board to set priorities based on latest developments in order to respond to changing needs and evolving threats, ENISA's activities do not fully meet the needs of all its stakeholders:
- ENISA's work programme is dominated by the interests of the Member States, and yet it is necessary to consider the longer-term perspective and the activities of other stakeholders in the cybersecurity area (such as other EU agencies or the private sector) to ensure continued relevance of the Agency
- ENISA's stakeholders strongly differ in their needs, making it difficult to meet them all. Some Member States (such as Germany, France or Sweden) have significant capacity and resources in the area of cybersecurity and rely on ENISA only for specific services. Other Member States (from Eastern and Southern Europe) are less experienced and rely more strongly on the expertise and capacity of ENISA. The Commission has their own needs and expectations with regard to the services that ENISA can provide to the different DGs. Additionally, industry stakeholders, including a high number of Small and Medium Enterprises (SMEs) are important actors in NIS and could also benefit from ENISA's activities

Effectiveness: In general, ENISA implements its tasks and achieves its set targets. ENISA has made a contribution to increased NIS in Europe through the four tasks presented in the table below, though there is room for improvement in relation to each.

Community building		Capacity building	
Achievements	Areas for improvement	Achievements	Areas for improvement
✓ Important contribution to enhanced cooperation between Member States and related NIS stakeholders, in particular between CERTs/CSIRTs	- Cooperation could be strengthened between ENISA and the Commission and other EU agencies, and with the private sector	✓ Contribution to enhanced capacities in the Member States, most notably in Member States with limited capabilities and resources in the area of cybersecurity ✓ Important activities include the Cyber Europe Exercises and trainings for CERTs/CSIRTs	- Capacity building with the private sector could be increased

---

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Expertise provision		Supporting development and implementation of policies	
Achievements	Areas for improvement	Achievements	Areas for improvement
✓ Important contribution by supporting CERTs/CSIRTs	- ENISA has not managed to become recognised as a centre of expertise or a reference point for other stakeholders, such as EU institutions or the private sector - High reliance on procurement of external expertise and limited resources available in-house	✓ ENISA has assisted the Member States and the Commission in developing and implementing policies	- ENISA is not consistently being involved by the Commission in all NIS-related activities

ENISA's contribution to NIS in Europe is limited by several key factors, including:
• The broad mandate under which a variety of tasks is to be covered, leaving limited scope to work on its own initiative and other than upon request
• The Agency's difficulties in attracting and retaining cybersecurity experts as staff members, due to various reasons including weak human resources procedures during the period under review
• The limited visibility of ENISA – the Agency is not sufficiently known across the EU and has not been able to establish a brand, unlike other EU agencies

Efficiency: ENISA has among the lowest budgets and levels of human resources compared to other EU agencies. In order to complete the various tasks set out in its mandate, ENISA has to be very efficient in the implementation of its budget and carefully consider where resources and working hours can be spent. The Agency develops a high number of publications every year and implements many other activities. Despite its small budget, the Agency has been able to contribute to targeted objectives and impacts, showing efficiency in the use of its budget.

In terms of efficiency, ENISA faces two main challenges:
• A number of administrative requirements set by the Commission which are the same for all EU agencies but weigh more heavily on smaller agencies
• A location split between Athens and Heraklion, requiring additional efforts of coordination and generating additional costs

Coherence: ENISA's activities are generally coherent with the policies and activities of its stakeholders, but there is a need for a more coordinated approach to cybersecurity at EU level. The potential for cooperation between ENISA and the European Commission, as well as other EU bodies, is not fully utilised. For example, the division of responsibilities between ENISA and CERT-EU should be clarified.

ENISA's activities are largely coherent with the work done at national level in the area of cybersecurity. Coherence is particularly strong between the CERTs/CSIRTs and ENISA. Some overlaps between ENISA's activities and those of Member States with strong cybersecurity expertise were identified, but Member States with less capacity and resources in the area of cybersecurity still benefit from its activities.

EU-added value: ENISA's added value lies primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related NIS communities. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. The added value of ENISA differs between Member States, depending on their cybersecurity capacities and resources. The Agency's activities of providing expertise and capacity building

represent important added value for Member States with few national resources dedicated to cybersecurity. This is less the case for Member States with more cybersecurity capacities.

Consequently, a discontinuation of ENISA would impact Member States differently. While Member States with strong cybersecurity capacities will be able to replace the services provided by ENISA at least to some extent, this will not be the case for Member States with fewer resources. The latter Member States rely more on ENISA's services in terms of capacity building, access to expertise and support in the implementation of policy and legislation. Cybersecurity crosses borders, so there is a need to build capacity to avoid weaker links that can impact on cybersecurity in the EU as a whole, as well as a need to provide a cross-EU response. It will not be possible to ensure the same degree of community building and cooperation across the Member States without a decentralised EU agency for cybersecurity; the picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA. Therefore, coordination at EU level is needed.

A potential discontinuation of ENISA would be a lost opportunity for all Member States. Most stakeholders were of the opinion that ENISA could take on a more important role in the EU cybersecurity landscape in the future, ensuring a common response capacity. This potential for the Agency to capitalise on future opportunities would be lost should it be discontinued.

SWOT analysis: Based on an analysis of the context – namely the evolution, since the last revision of ENISA's mandate in 2013, of the cybersecurity and digital privacy landscape - the evaluation study provides an assessment of the main strengths and weaknesses of ENISA, and the opportunities and threats in the new cybersecurity and digital privacy landscape. These are presented in the figure below.

Table 2: ENISA's SWOTs

Strengths	**Weaknesses**
- Neutral, facilitator, free of political bias or commercial interests - Recognised support to Member States in capacity building & capability development to strengthen resilience to cyber-threats - Acknowledged collaboration & community building reaching wide range of actors, incl. Member States, industry, EU bodies etc. - Horizontal expertise, "landscape overview" of Member States cybersecurity policies	- Low visibility for various reasons: lack of expertise, weak communication/marketing and limited self-assertion within the EU cybersecurity policy landscape - Lack of a long-term, strategic vision - Recruitment difficulties - Reduced efficiency due to split location - Distance to EU decision makers in Brussels - Lack of financial and human resources to make a difference
Opportunities	**Threats**
- Growing need for synergies between information and communication technology (ICT) operators to ensure concerted and collaborative NIS policy actions - NIS Directive bears the potential to strengthen ENISA's role in EU cybersecurity policy - There is an acknowledged need and demand of stakeholders to strengthen awareness raising of cybersecurity - Stronger support in the community is evolving for ICT standardisation and certification	- Policy fragmentation at EU level and diverging policy priorities in EU Member States constrain ENISA's scope of action - Rapidly evolving and complex threat landscape involving multiple disciplines create new vulnerabilities, e.g. Internet of Things (IoT) - Lack of overall (technical) talent in the field of cybersecurity aggravates ENISA's recruitment difficulties

In conclusion, the following **key issues** have been identified as requiring action to improve ENISA's relevance, effectiveness, efficiency, coherence and added value in the future and ultimately help it contribute to increased NIS in the EU: Weak institutional and legal framework for cybersecurity in the EU – Cybersecurity is primarily seen as an area of national competence, while in reality it is an issue that transcends borders

- *Fragmentation of cybersecurity policy at EU level* – The fragmentation of cybersecurity policy is due to a number of EU-level actors in the area of cybersecurity and insufficient coordination

between them. One important factor here is the division of responsibilities between ENISA and CERT-EU.

- *Limitations for ENISA due to its size* – ENISA has difficulties to make an impact in the vast field of NIS as it has only limited human and financial resources to meet a broad mandate.
- *Limited visibility* – ENISA has not managed to develop a strong brand name and is not seen as a point of reference at European level for cybersecurity.
- *Not perceived as a proactive, visionary Agency* - ENISA's broad mandate makes it reactive to fulfilling the needs of as many stakeholders as possible, but this means that it loses focus. ENISA is not able to use its own knowledge to set work priorities due to the Member State dominance of the work programme.
- *A mandate that is not aligned with cybersecurity needs* – Cybersecurity threats have become a permanent issue in the EU and ENISA has been allocated long-term responsibilities (e.g. under the NIS Directive) which call for a permanent mandate.
- *ENISA does not sufficiently respond to the needs of all its stakeholders* – Under the current governance structure, the needs of the private sector are not sufficiently heard and thus are not adequately reflected in the Agency's work programmes.
- *ENISA should expand its activities to better respond to stakeholder needs* – There is a request by stakeholders (although not unanimous) to ensure a coherent ICT certification and standardisation system in the EU. Member States with fewer resources and expertise require additional support in receiving information on and assessing cybersecurity threats in order to respond to attacks.

Despite these issues, there is significant potential for ENISA, if sufficiently mandated and supported in terms of financial and human resources, to make a contribution to increased NIS in the EU. There is a clear need for cooperation and coordination across different stakeholders and ENISA as a decentralised EU agency is in the position to ensure a coordinated approach to cyber threats in the EU.

Options for the future of the Agency

Based on the key issues presented above – as derived from the findings and conclusions of the study - four options to review the current mandate of ENISA were developed. They are presented in Table 3 below, highlighting the specific factors for change that could be implemented under each of the options.

Table 3: Options for the future of ENISA

Option	Factor for change
Option 0: Baseline, maintain the status quo This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation[3] and Telecoms Framework Directive[4] would need to be taken into account.	**Revise ENISA's mandate to make its new tasks as per recent/upcoming legislation more specific:** • Involvement in Cooperation Group as required under the NIS Directive • CSIRT Network Secretariat • Electronic communication code, recital 92 (Telecoms Framework Directive) • eIDAS
Option 1: Expiry of ENISA's mandate (terminating ENISA) This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive	N/A

---

[3] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[4] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

and bilateral or regional ties at Member State level.	
Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate) This option concerns making significant revisions to ENISA's mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.	**Strengthen ENISA's operational role:** • Provide periodic threat intelligence and ad hoc alerts • Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level • Provide emergency cybersecurity response
	Strengthen ENISA's role in policy development and implementation: • Render the consultation of ENISA by the Commission in cybersecurity matters obligatory • Formally involve ENISA in the Connecting Europe Facility • Establish regular meetings between ENISA and other agencies/international organisations
	Make ENISA's mandate permanent
	Strengthen ENISA's governance structure: • Increase the role of the Permanent Stakeholders' Group (PSG) • Allow ENISA more flexibility in the determination of its work priorities
	Include a role for ENISA in EU-level standardisation and certification: • Support the EU ICT Security Certification Framework • Support ICT security standardisation
	Strengthen ENISA's position relative to research and innovation: • Take part in programming implementation • OR Take part in programming in an advisory role • OR Benefit from EU research and development funding
	Increase ENISA's visibility: • Establish a liaison office in Brussels • Create a dedicated communications team within ENISA
Option 3: European Agency with full operational capabilities (Establish a European Centre of Cybersecurity) This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.	**Create an EU cybersecurity umbrella:** • Such an umbrella would encompass ENISA and CERT-EU
	Create a virtual European CSIRT: • Coordinate CSIRT Network operations • Produce real time situational awareness and dynamic threat intelligence feeds • Maintain and provide own cybersecurity incident response capacity to public and private sector
	All factors related to Option 2 could be fulfilled under Option 3.

1. INTRODUCTION

This is the final report for the "Study on the Evaluation of the European Union Agency for Network and Information Security (ENISA)". The study was implemented between November 2016 and July 2017.

The study aims to support the Commission in evaluating the impact, effectiveness, efficiency, relevance, coherence and value added of ENISA and its working practices, and prepare the ground for a possible revision of the mandate of the Agency. The Commission is evaluating ENISA based on Article 32 (1) of ENISA's Regulation (Regulation No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004) which requires the Commission to "commission an evaluation to assess, in particular, the impact, effectiveness and efficiency of the Agency ad its working practices. The evaluation shall also address the possible need to modify the mandate of the Agency and the financial implications of any such modification."

As such, the study contains both a summative dimension, looking back at the achievements of the 2013-2016 period, as well as a more formative, forward-looking aspect, as further described below:

- Summative dimension: This aspect of the study assesses the results achieved by the Agency having regard to its objectives, mandate and tasks as set out in the ENISA Regulation.
- Formative dimension: This forward-looking assessment is based on the evaluation of the current positioning of ENISA with respect to other EU and national bodies in meeting the needs of its constituency and the new challenges engendered by the evolving cybersecurity and digital privacy landscape. The study provides recommendations on the possible need to modify the mandate of the Agency and assesses the financial implications of such modifications.

This introductory section presents the structure and content of this report and provides a brief overview about ENISA and the Agency's work, including its intervention logic.

1.1 Structure and content of the report

This report is structured in four main parts. The introduction is followed by information about the methodology applied to implement the study. The third part of the report presents the findings of the study, which are structured according to the evaluation criteria, i.e. relevance, effectiveness, efficiency, coherence and EU-added value, and concludes with an analysis of ENISA's strength, weaknesses, opportunities and threats, a so-called SWOT analysis. The fourth and final part of the study presents conclusions on ENISA's key achievements and the most pressing issues at strategic level and at the level of the Agency, before going on to discuss potential options for the future. The specific factors for change of the options are discussed, including an assessment of the costs of their implementation, their added value and coherence.

Part	Heading
1	Introduction
2	Methodology
3	Findings
4	Conclusions and recommendations

The report includes the following appendices:

Appendix	Heading
1	Evaluation question matrix
2	Bibliography
3	Survey questionnaires
4	Positioning exercise
5	Comprehensive SWOT table

1.2 About ENISA

ENISA is the EU agency for network and information security. It was established in 2004 by Regulation (EC) No 460/2004. Since then, ENISA's mandate has been reviewed once and extended several times. The latest changes were implemented with Regulation (EU) No 526/2013 (hereafter "the Regulation"). The Agency is located in Greece with its seat in Heraklion on Crete and an operational office in Athens.

1.2.1 ENISA's mission tasks and activities

The Agency's activities consist in providing advice and recommendations, data analysis, as well as supporting awareness raising and cooperation by the EU bodies and Member States. Building on national and Community efforts, the Agency is a centre of expertise in this field. ENISA uses its expertise to improve cooperation between Member States, and between actions from the public and private sectors, as well as to support capacity building.

ENISA's Strategic Objectives (from 2015[5]) are presented in the figure below.

Figure 1: Strategic Objectives of ENISA
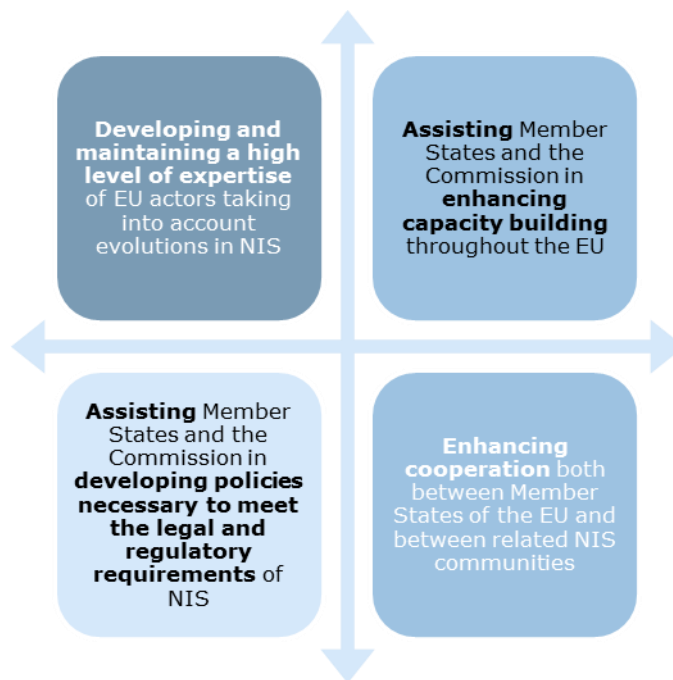
Source: Ramboll Management Consulting based on ENISA website

In order to achieve its Strategic Objectives, ENISA delivers four key tasks in accordance with the Regulation, namely:
- ✓ Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- ✓ Collecting and analysing data on security incidents in Europe and emerging risks.
- ✓ Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.

---

[5] There was a shift from work streams to strategic objectives in 2015.

   ✓ Raising awareness and strengthening co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field.

In addition, ENISA undertakes European Network and Information Security (NIS) Good Practice Brokerage activities, which are based on the concept of the exchange of good practices between EU Member States at the area of NIS on a pan-European scale. ENISA acts as a broker in the European NIS 'marketplace' to facilitate the exchange of good practices by:

- supporting co-operative meetings with Member States and other stakeholders;
- assisting in the exchange of experts between Member States;
- supporting the exchange of good practice material;
- contributing with its expertise to co-operative projects.

ENISA mainly conducts the previously mentioned tasks through four activity areas: Computer Emergency Response Teams/ Computer Security Incident Response Teams (CERTs/CSIRTs), Critical Information Infrastructure Protection (CIIP) and Resilience, Identity & Trust and Risk Management.

1.2.2 ENISA's organisational structure

The organisational structure of ENISA is laid down in the Regulation which states that the Agency comprises an Executive Director and staff, a Management Board, an Executive Board and a Permanent Stakeholders' Group (PSG). Each of these is described in further detail below.

The Executive Director is appointed by the Management Board and is responsible for managing the Agency and performs his/her duties independently. He/she also establishes **ad hoc working groups**, in consultation with the PSG, which are composed of experts. The ad hoc working groups are addressing specific technical and scientific matters.

The Management Board is composed of representatives of the Member States and the Commission. Tasks of the Management Board include the establishment of the budget, verification of its execution, adoption of the appropriate financial rules, establishment of transparent working procedures for decision-making by the Agency, approval of the Agency's work programme, adoption of its own rules of procedure and Agency's internal rules of operation, appointment and removal of Executive Director. The Management Board will adopt the Agency's internal rules of operation on the basis of a proposal by the Commission. The Management Board ensures that the Agency carries out its tasks under conditions which enable it to serve in accordance with the founding Regulation

The PSG is set up by the Management Board, acting on a proposal by the Executive Director, for a term of office of 2.5 years. For the period 2015-2017, the PSG is composed of "nominated members" and of members appointed "ad personam", representing in total 23 members from all over Europe. The 20 members appointed "ad personam" constitute a multidisciplinary group from industry, academia, and consumer organisations and have been selected upon the basis of their own specific expertise and personal merits. Three "nominated members" represent national regulatory authorities, data protection and law enforcement authorities. The role of PSG is to advise the Executive Director on the development of the Agency's work programme, and on ensuring the communication with the relevant stakeholders on all related issues.

In line with the operational and horizontal objectives of the Agency, ENISA's organisational structure was reorganised in December 2013, as depicted in the figure below.

Figure 2: Organisational chart of ENISA (2013 to late 2016)
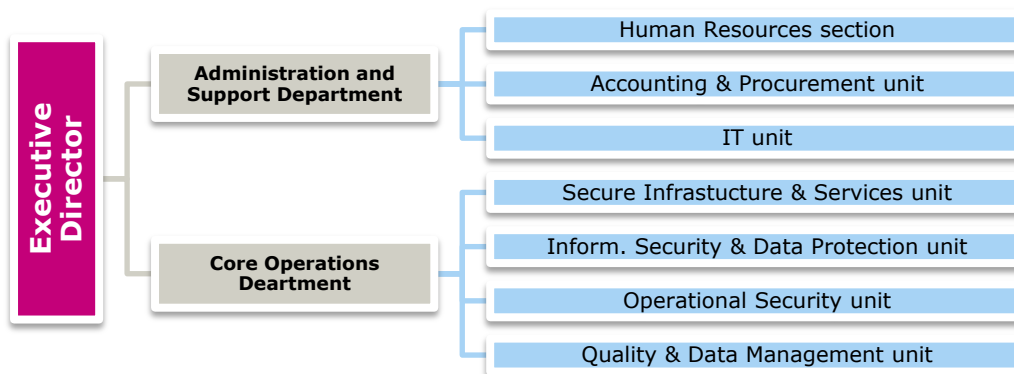
Source: ENISA website, Structure and Organisation

ENISA's organisational structure was changed in late 2016 to include an "Executive Director's Office" and the units within the core operations and administrative departments were reorganised; the split between operations and administration (which from end 2016 also covers "stakeholder relations") was maintained. The previous structure of ENISA has been presented here in line with the scope of this evaluation (2013-2016).

1.2.3   ENISA's stakeholders

Engaging with, working with and assisting its stakeholders, is a key factor for ENISA's success and the overall mission of contributing to the security of the EU internal market. Therefore maintaining relationships with these stakeholders through formal and informal channels is one of the main tasks of ENISA. ENISA has importantly set up and continues to maintain a formal group of liaison officers, called **the Network of National Liaison Officers (NLOs)**. This network should be highlighted since, though not formally based on the ENISA Regulation, it is of great value to ENISA as the NLOs serve as ENISA's key points of reference in 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 and its network consists of (at least) one NLO per Member State. Typically an NLO works in the field of NIS, either in the public sector (ministry), or the IT/telecom sector. In coordination with the Managing Board representative, it may be decided to appoint multiple NLOs for one country – particularly when the country is large or when there are multiple distinct communities (private, public, etc.).

In addition, ENISA has established relations with a wider stakeholder group. These include industry organisations, end user organisations, EU bodies, International Organisations, research and academia, third countries, etc. This open and growing network of stakeholders is essential to the Agency's goals in identifying emerging risks and forging new insights to help Member States and private sector organisations through access to NIS experts. Figure 3 shows a map of ENISA's stakeholders who together strengthen to Agency's capacity to prepare for challenges in a proactive and increasingly professional manner by building novel public and private sector partnerships.

Figure 3: ENISA's stakeholder map
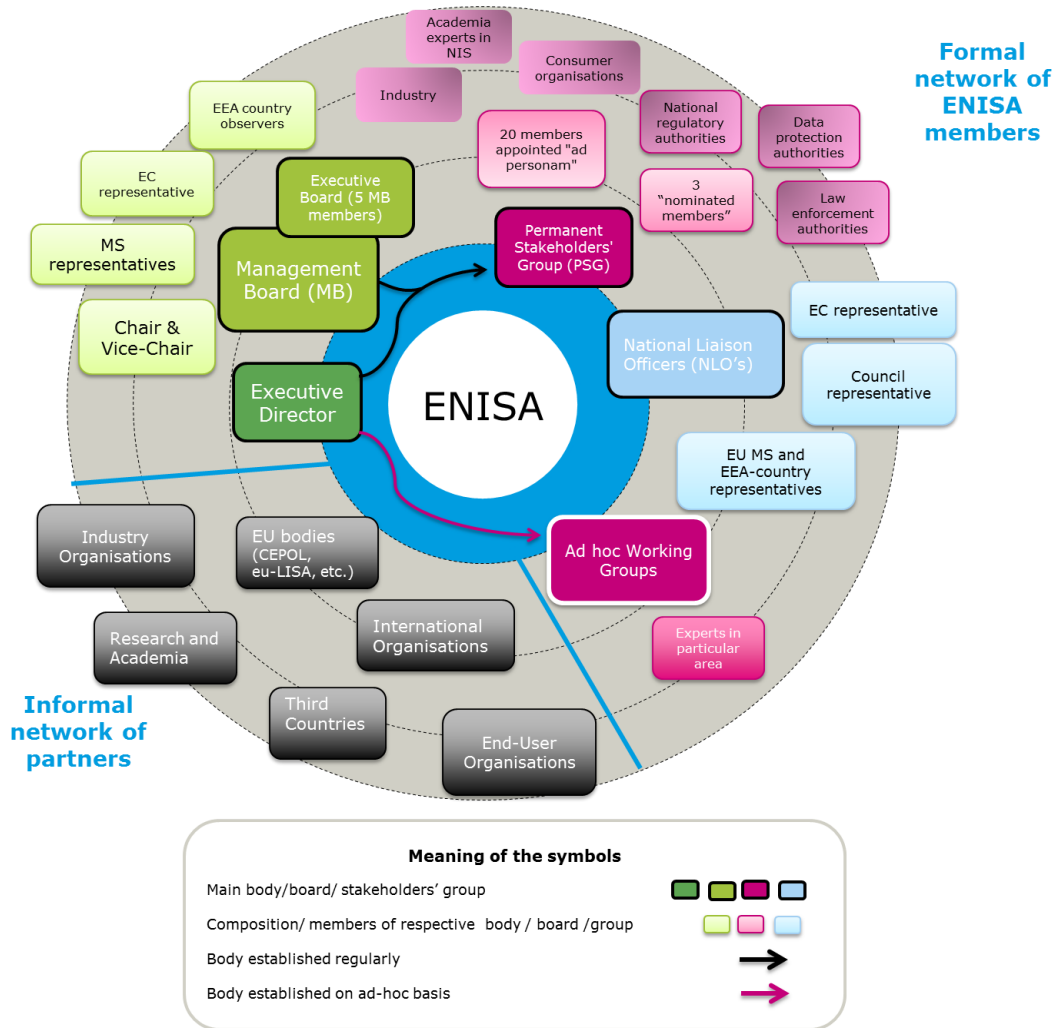
Source: Ramboll Management Consulting based on ENISA website, *Structure and Organisation, Stakeholders Relations*

1.2.4 Intervention logic

The figure below presents the intervention logic for ENISA as an organisation based on the Regulation, which shows how its four key areas of activity are intended to deliver the Agency´s Strategic Objectives and impacts. This intervention logic is a systematic and reasoned description of the casual links between the Agency's activities, outputs, outcomes, results and impacts, as well as the key external factors affecting the implementation, results and impact of ENISA's activities. It helps to understand the objectives of the Agency as a whole and its specific tasks.

This study has used the intervention logic as a basis to assess ENISA's effectiveness in achieving targeted results and impacts based on the implemented activities.

Figure 4: Intervention Logic of ENISA as an organisation
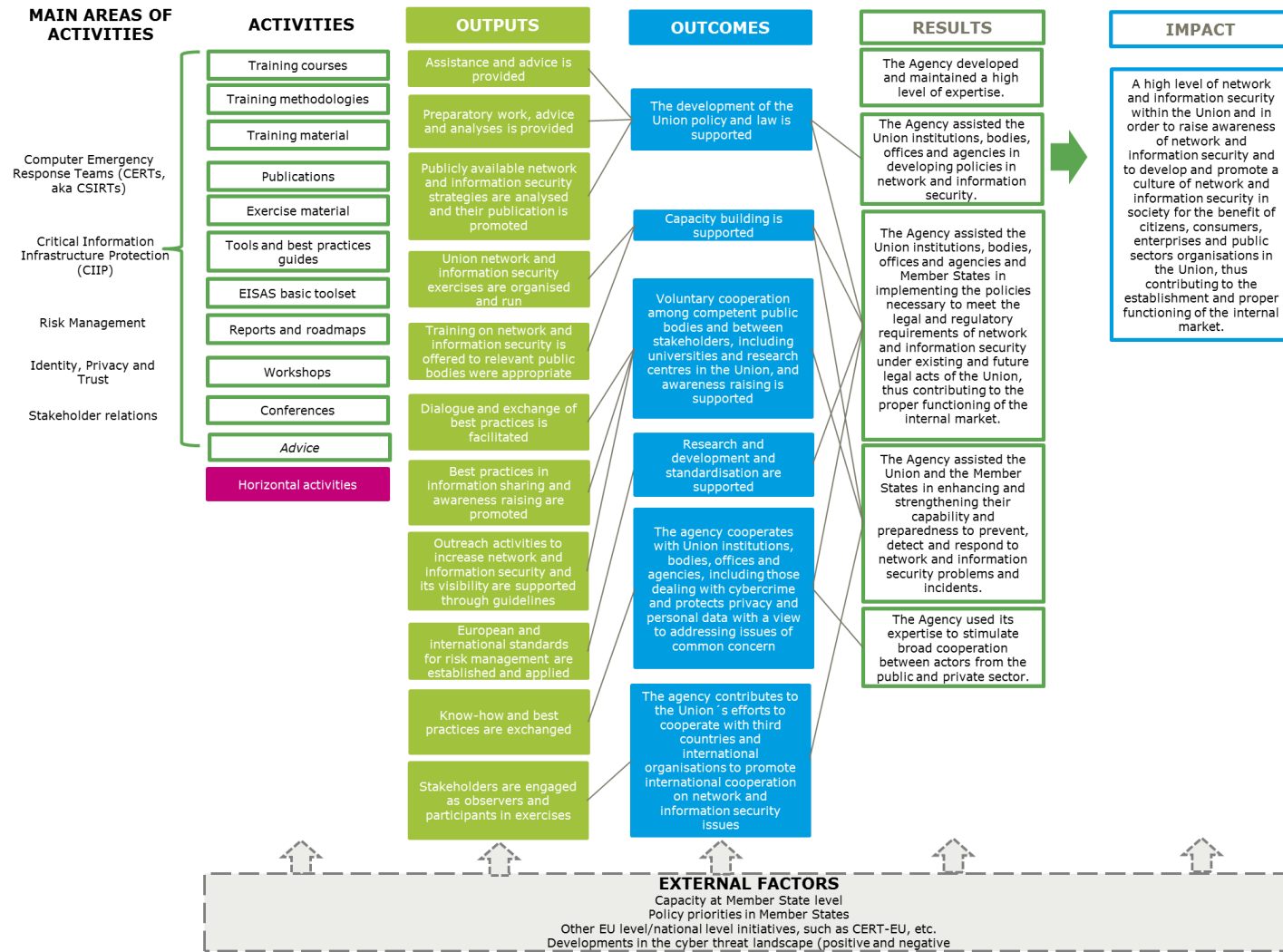
Source: Ramboll Management Consulting based on Regulation (EU) No 526/2013

2.   METHODOLOGY

The purpose of the evaluation study was to support the Commission in evaluating the impact, effectiveness, efficiency, relevance, coherence and value added of ENISA and its working practices, and prepare the ground for a possible revision of the mandate of the Agency. To do so, four different analytical tasks were implemented. As part of the summative (backward-looking) part of the study, the performance of ENISA (i) and its governance and organisational structure (ii) were assessed, and ENISA's positioning with regard to other EU agencies and bodies and national authorities was also analysed (iii). As part of the formative (forward-looking) dimension of the study, ENISA's SWOTs in a new context have been identified.

This part of the study presents an overview of the methodology employed for the evaluation of ENISA, by detailing the data collection activities and analytical tasks that have been implemented. The study answers a set of 46 evaluation questions based on the Commission's evaluation roadmap for ENISA[6]. A complete evaluation question matrix is presented in Appendix 1.

The methods chosen to evaluate ENISA in accordance with the requirements of this study and to respond to the evaluation questions are presented in Figure 5 below.

Figure 5: Methodology of the study
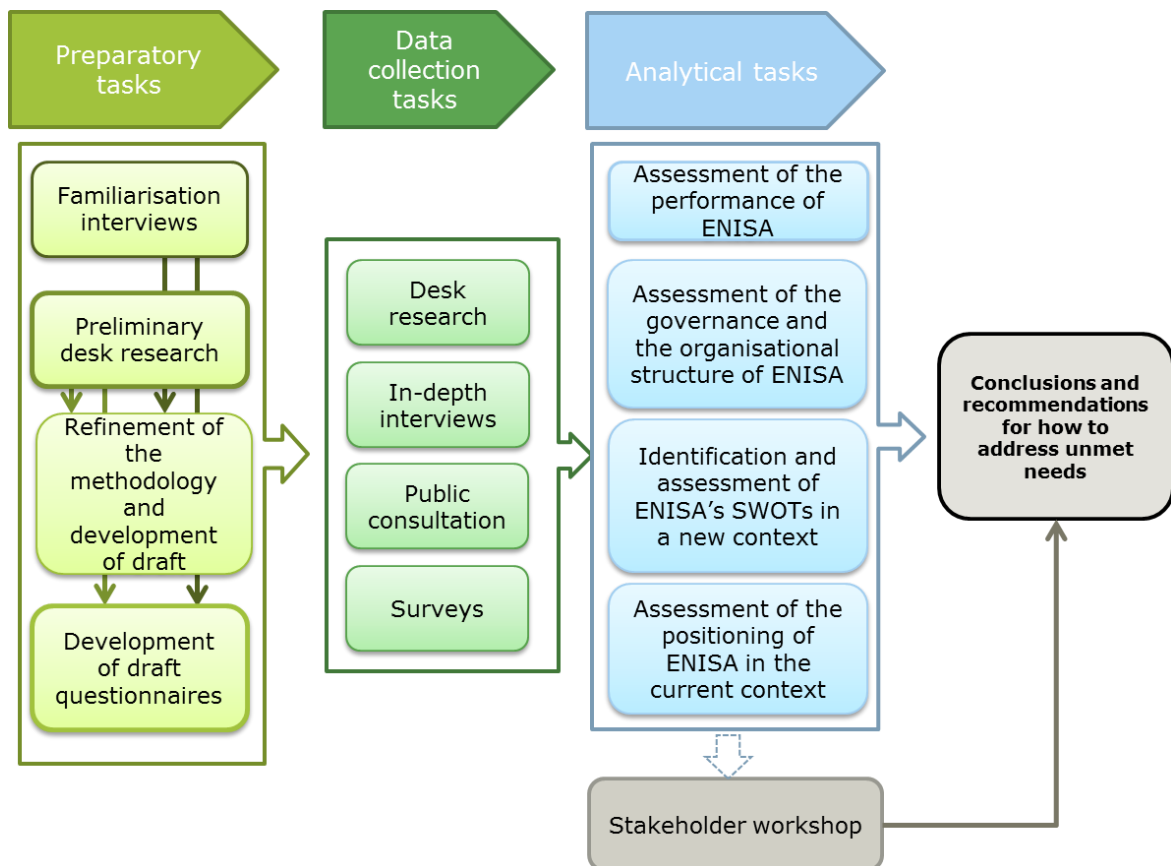
Each of the tasks is described in further detail below.

2.1   Preparatory tasks

The preparatory tasks were used to set up the methodology and tools for the study and ensure a common understanding of the scope and objective of the evaluation between the European

---

[6] European Commission (2016): Evaluation Roadmap – Evaluation of the European Union Agency for Network and Information Security (ENISA)

Commission and the study team. For this purpose, five **familiarisation interviews** were conducted with members of the European Commission DG Communications Networks, Content and Technology (DG CNECT) and DG for Informatics (DIGIT), and with the Computer Emergency Response Team for the EU institutions, CERT-EU. **Preliminary desk research** allowed for the identification of the policy, legal and academic documents of relevance to the study. Based on the understanding gained of ENISA and the purpose of the evaluation, the **methodological approach was refined**, including a finalisation of the evaluation question matrix and **data collection tools were developed**.

2.2 Data collection tasks

The data collection included a desk review of relevant literature and the consultation of different stakeholders. In-depths interviews with a wide range of ENISA's stakeholders, staff and management were conducted, surveys specifically targeted at ENISA's staff and management and at CERTs/CSIRTs were implemented, and an open public consultation allowed all EU citizens and organisations to contribute to the study. At the end of the data collection and after some analysis, a workshop was held with ENISA's stakeholders in order to validate the findings and preliminary conclusions. Through these various means, a wide range of stakeholders were consulted, ensuring the representativeness of the findings presented in chapter 3.

2.2.1 Desk research

The study is based on a variety of secondary sources which fed into all of the analytical tasks. These sources include legal sources on relevant EU legislation, EU strategies and policy documents, reports published by ENISA on programming and reporting, previous evaluations conducted for the Agency and a number of key papers and reports on the issue of cybersecurity in Europe.

A full list of documents is provided in Appendix 2.

2.2.2 Consulted stakeholders

The data collection among stakeholders included the following activities: in-depth interviews, an open public consultation, a survey among ENISA's staff and management as well as direct stakeholders (members of the Management and Executive Board of the Agency, NLOs and the PSG), a survey among CERTs/CSIRTs and a stakeholder workshop. Table 4 below presents an overview of the different formats used to involve stakeholders in the study.

Table 4: Format and purpose of stakeholder consultation tools

Consultation tool	Format	Purpose
Interviews (49 interviews conducted)	In-depth interviews over the phone or in person	• Gather information on ENISA's performance (ENISA's staff and management, its direct stakeholders and the European Commission and Parliament) • Collect data on ENISA's governance structure (staff and management, direct stakeholders) • Gather views on ENISA's SWOTs (all stakeholders) • Collect information to understand ENISA's positioning (other EU agencies and bodies)
Survey to ENISA staff and direct stakeholders (88 participants)	Online survey to ENISA's staff, the Management and Executive Board of the Agency, NLOs and the PSG. Current, as well as former, Management Board members and NLOs were contacted. A total of 199 stakeholders were invited to participate.	• Gathering views on the effectiveness and efficiency of ENISA's governance, organisational set-up and working practices
Survey to CERTs/CSIRTs (34 participants)	Online survey sent out to CSIRT Network, including CSIRT representatives from all 28 Member States and CERT-	• Gathering views on cooperation and coordination between ENISA and the CERTs/CSIRTs • Providing input to assess the coherence and complementarity between ENISA's activities and those

	EU.		of the CERTs/CSIRTs		
Open public consultation (90 participants)	Questionnaire available online between 18 January and 12 April 2017	• Contribution to the assessment of ENISA's performance, the analysis of SWOTs, and to the development of recommendations for the future			
Workshop (43 participants)	Implemented following the analytical tasks. Held on the premises of the Commission in Brussels on the 22nd of March 2017. Presentation of preliminary findings, conclusions and options.	• Gathering participants' views on the results of the evaluation and to discuss possible options for the future of cybersecurity in Europe • Validation of findings			

Through the different data collection tools more than 300 stakeholder contributions were received from across various groups as presented in Table 5 below (individual stakeholders may have contributed to the evaluation through different data collection tools).

Table 5: Stakeholders reached per data collection tool

Target group	Type of stakeholder	Number of interviewees	Number of survey respondents	Number of participants to the Open public consultation	Number of workshop participants[7]
Direct stakeholders	Members of ENISA's Management Board and Executive Board	8	19	10	12
	PSG	2	13	3	5
	NLOs	2	12	1	
ENISA's users and advisors	European Commission	6			
	European Parliament	3			
	Other EU agencies and bodies	5			4
	CERTs/CSIRTs	3	34		2
	National cybersecurity authorities	1		9[8]	5
	Industry representatives (private enterprises or business associations)	4		26[9]	9
	Civil society organisations or individuals	2		26[10]	2
	Research or academic institutions			10	2
	Consultants			5	
	Authorities from third countries	1			
ENISA staff and management		12	44		2
Total		**49**	**122**	**90**	**43**

Across the data collection tools (interviews, open public consultation, workshop), Management Board members of at least 19 Member States were involved in the study.[11] These cover a spectrum of smaller and larger Member States and of different regions.

In addition to the data collection tools presented in the tables above, seven interviews were conducted with national authorities and policy-makers in the latter stage of the evaluation, focussing on the forward looking part of the study and seeking to further operationalise the options under consideration for the future of the Agency. These include Member State representatives and their alternates to ENISA's Management Board, members of ENISA's Executive Board,

---

[7] Participants from the Commission have not been included in the list of participants and are thus not included below.

[8] Including a position paper received from France

[9] Including one position paper from a UK based business association

[10] This includes 20 respondents who indicated to answer in their personal capacity.

[11] The contributions to the surveys were anonymous. It cannot be verified which Member States were covered.

CERTs/CSIRTs and national cyber security authorities, as well as management staff from ENISA, representatives of DG CNECT and from the private sector.

Further information on the data collection methods can be found in Appendix 3 including the questionnaires used to the two surveys.

2.3   Analytical tasks

The study involved four analytical tasks which were used to reach conclusions and recommendations for the revision of ENISA's mandate and to suggest potential improvements, as presented in Table 6.

Table 6: Analytical tasks and their purpose

Analytical task	Purpose
Assessment of ENISA's performance	• Assessment of effectiveness, efficiency, relevance, coherence and EU added value of the work undertaken by ENISA and its working practices over the 2013-2016 period • Review of ENISA's intervention logic to establish the extent to which ENISA's activities and outputs have contributed to the expected results and impacts • Assessment of whether ENISA has been able to establish itself as an EU-wide centre of expertise and reference point for stakeholders • Assessment of the degree to which the Agency's priorities, as set out in its work programmes, are in line with the needs of the time and the degree of the Agency's flexibility to respond to unforeseen needs
Assessment of the governance and organisational structure of ENISA	• Assessment of how the current, governance, internal organisational structure of ENISA, location and human resources policies and practices contribute to efficiency in and effectiveness of the work of the Agency • Benchmarking exercise comparing ENISA's governance and organisational structure to that of other EU agencies and organisations
Assessment of the positioning of ENISA in the current context	• Assessment of how ENISA is positioned vis-à-vis a sample of other EU and national bodies working on cybersecurity and digital privacy on the basis of the services offered and the needs expressed by the Agency's stakeholders • Mapping of the services provided by ENISA and of a selection of other EU and national bodies against identified needs to highlight existing complementarities and potential overlaps between the offered services • Development of a positioning map
Identification and assessment of ENISA's SWOTs in a new context	• Identification and assessment of ENISA's strengths, weaknesses, opportunities and threats (i.e. current status / position) in the context of the new and evolving cybersecurity challenges and digital privacy landscape and ENISA's current mandate • . • Based on all data collection tasks and builds on the analysis conducted as part of the other analytical tasks • Involvement of a panel of cybersecurity experts covering the policy, legal and technical aspects of the area in this task

The analytical tasks included a benchmarking and a positioning exercise. The sample of EU agencies and bodies selected for these two exercises is presented below.

The EU agencies and bodies covered under the **benchmarking exercise** are presented in Table 7 below. Organisations were selected based on similarities in their work areas and activities with those of ENISA, or in their size to ENISA in terms of number of staff and budget.

Table 7: Organisations selected for the benchmarking

Organisation	Reason for selection
Europol – European Cybercrime Centre (EC3)	Similarities in the work areas and activities
European Union Agency for Fundamental Rights (FRA)	Availability of data
Office of the Body of European Regulators for Electronic (BEREC office)	Similarities in the work areas and activities
European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)	Similarity in the activities
European Union Agency for Law Enforcement Training (CEPOL)	Similarity in the activities and similarity in terms of staff number and budget
European Fisheries Control Agency (EFCA)	Similarity in terms of staff number and budget

For the positioning exercise, ENISA's activities were mapped across four tasks: enhancing cooperation, develop and maintain a high level of expertise, enhancing capacity building and developing and implementing policies. Sub-categories of these were developed to understand the more specific tasks that were implemented. The complete mapping of ENISA's services and the full positioning exercise is attached in Appendix 4. The services were then compared to the sample of other EU and national bodies presented in Table 8 below. These organisations were contacted to provide information on their activities. The completeness of the responses received from these organisations varied and in a few cases no responses were received despite numerous follow ups per email and over the phone. As a consequence, parts of the positioning exercise only rely on desk research.

Table 8: Organisations covered under the positioning exercise

Organisation	Status
CERT-EU	Input received
Commission Joint Research Centre (DG JRC) Science Hub	Input received
EC3	Assessment made based on desk review
Netherlands National Cyber Security Centre (NCSC)	Input received with no assessments of overlaps or complementarity
French National Cybersecurity Agency (ANSSI)	Assessment made based on desk review
Spanish National Institute for Cybersecurity (INCIBE)	Input received with no assessments of overlaps or complementarity

The aim of the **positioning exercise** was to compare ENISA to organisations implementing similar activities in order to assess ENISA's coherence and identify any potential overlap. Therefore, EU bodies and agencies, and organisations from Member States where the expected potential for overlap was high were selected. Results from the annual evaluations of ENISA in 2014 and 2015 showed that this was the case for Member States' cybersecurity organisation with comparably high human and financial resources and experience in the field of cybersecurity. The selected national organisations were not intended to be representative of all Member States. The needs of Member States with fewer resources and experience in cybersecurity were assessed through different means of data collection and analysis.

As a first step in the **analytical process**, the data gathered through the in-depth interviews, the surveys and open public consultation in relation to the operationalised evaluation questions (see the evaluation matrix in Appendix 1) was analysed, comparing and contrasting the views of different stakeholder types from the same data source.

In a second step, the desk-based analysis was triangulated with the data collected through the different stakeholder consultations, allowing for responses to be drafted in relation to the evaluation questions. On this basis, substantiated conclusions were drawn. The conclusions provide an overall judgement of the effectiveness, efficiency, relevance, coherence, EU added value and impact of ENISA and with regard to the future needs and challenges. The preparation of conclusions and, subsequently, the recommendations is based on four pillars:

- Transparent use of all evidence collected
- Validation of conclusions, notably through the stakeholder workshop and an expert panel
- Recommendations flowing directly from conclusions
- Validation of recommendation and their expected impacts, notably through the stakeholder workshop and an expert panel.

2.4 Developing conclusions and recommendations

Against the responses to the evaluation questions reached through the analytical tasks, the most pressing issues at the strategic level and at the level of the Agency were identified and options for the future of ENISA developed. Efforts were made to ensure that a clear and direct link was made between the conclusions and recommendations, enabling the tracking of the reasoning from the analysis carried out in relation to the evaluation questions through to the options for the future. By so doing, it is ensured that the extent to which the recommendations are based on opinion, analysis and objectively verifiable evidence is clear.

An estimation of the costs related to each of the factors for change under a given option derived from the results of the evaluation was developed. The assessment was made on the basis of existing standard costings for the period under review (e.g. for full-time equivalents (FTEs), given activities) and took into account additional start-up costs, where relevant. Furthermore, the EU added value and coherence of the suggested tasks was assessed.

2.5 Challenges and limitations

The evaluation study presented a number of challenges, often relating to the availability of data. In the following, the main challenges are outlined, together with an explanation of how they were dealt with in the evaluation process.

Table 9: Challenges in the evaluation process

Challenge		Solution / Mitigation strategy
Benchmarking	For the benchmarking exercise other EU agencies and bodies were asked to provide data on their set-up (e.g. numbers of staff, vacancies) and on their outputs (e.g. numbers of publications). The completeness of responses received from the selected bodies varied and in a few cases no responses were received. Consequently, only limited data was available for the benchmarking exercise and not all foreseen comparisons could be made. It has not been possible to compare: • percentage of administrative staff and the percentage of operational staff • turnover of the senior management • number of management and executive board meetings (only compared for three agencies) • approach to the use of procurement or external expert groups • budget used for procurement of study • budget allocation to publications • number and costs of publications, trainings, awareness raising events	In response to the difficulties experienced in collecting the quantitative data originally intended, additional efforts were made to reach out to further agencies and, where possible, additional secondary data sources were employed in order to compare ENISA against. The main sources were the European Commission: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III and Court of Auditors (2016): Summary of results from the Court's annual audits of the European Agencies and other bodies for the financial year 2015; additionally annual reports of the relevant agencies were used. Despite these efforts, it was not possible to compare ENISA to the other agencies with regard to achieved outputs (such as publications, trainings, events). Moreover, while the scope of the evaluation is 2013-2016, the data which was judged most complete and comparable was used for the analysis. Therefore, there are some variations in the years reported on.
Positioning	These organisations selected for the positioning exercise were contacted to provide information on their activities (through an interview and by completing a data sheet). The completeness of the responses received from these	Data collected through the interviews and desk based research on the activities of the selected national and EU organisations was conducted to respond to the limited data received directly from the organisations covering the concrete points under the positioning exercise.

Challenge		Solution / Mitigation strategy
	organisations varied and in a few cases no responses were received despite numerous follow ups per email and over the phone.	Consequently, some of the assessments presented in the positioning exercise are based on desk research and the interviews but have not been triangulated with input from the organisations themselves in the form of the foreseen data sheet. The concerned organisations were not directly asked about their positioning at the detailed level of the data sheet. Therefore they may have a different understanding of their overlaps and complementarities with ENISA.
Assessing outputs and results	For the response to several evaluation questions, the use of the Agency's key performance indicators (KPIs) and was foreseen (for example for evaluation question 31 (EQ31)). ENISA has not been able to provide the requested data to implement the foreseen assessments. The key impact indicators (KIIs) of the Agency set in the annual work programmes and reported upon in the annual activity reports change from one year to the next. This limited the possibility to implement a comparison of the Agency's outputs and results over the entire period of 2013-2016.	Without the quantitative data on outputs and results the evaluation relied on the qualitative feedback collected through interviews, surveys and the open public consultation. Where available data from the evaluations of ENISA's activities in 2014 and 2015 has been introduced to the study.
Vested interests of stakeholders	As outlined in this section of methodology, the study relied to a large extent on stakeholder contributions. These stakeholders (in particular ENISA's staff and management and the direct stakeholders) may have vested interests in the future of the Agency. Therefore, a critical assessment of contributions needs to be made.	The analysis included triangulation of the data across different stakeholder groups and across the data collection tools. For example, the surveys and the interviews which primarily covered views from ENISA's staff, management and direct stakeholders were considered against the open public consultation results and the workshop where a broader scope of stakeholders have been reached.
Assessment of the costs related to the options	The assessment of the cost of the options identified needed to be based on a number of assumptions.	In order to establish as realistic assumptions as possible, the options were operationalised and a variety of stakeholders were consulted (i.e. Commission, ENISA, industry, Member State representatives) and external sources employed where relevant.

3. FINDINGS

This chapter presents the findings of the evaluation study. It presents responses to the evaluation questions listed in Appendix 1. The findings are based on the different data collection tools employed, as described in chapter 2.

The chapter is structured as follows:
- The first section presents an overview of the key findings of the study
- The second section presents the detailed findings and conclusions of the study, including the results of the three of the analytical tasks, namely the assessment of ENISA's performance; the assessment of ENISA's governance and organisational structure, and the assessment of ENISA's positioning.
- Finally, the third section presents the results of the SWOT analysis.

These three sections are structured according to the evaluation questions. In order to assist the (busier) reader, a concluding sentence has been highlighted at the top of each paragraph and the findings that support it are presented below it. Moreover, to allow readers to get a quick understanding of the main conclusions, a box summarising the main conclusions for each question can be found at the end of each subsection. Section 3.2 is structured according to the evaluation criteria: relevance, effectiveness, efficiency, coherence and EU added value. Here conclusions can be found for each of the evaluation criteria, as well as for the evaluation questions at a more detailed level.

The conclusions on each of the evaluation criteria include a short comparison of the assessment made for the 2013-2016 with that of ENISA in 2009 and 2010 based on an evaluation of all EU agencies including ENISA in 2009[12] and an impact assessment of changes to ENISA's mandate in 2010[13]).

As important stakeholders of ENISA's work and in the decision making on the future of the Agency, Member States' opinions have been highlighted throughout the report. It should be noted that, based on the different data collection tools, different types of Member State representatives have been consulted (see also section 2.2.2). In the context of the interviews, "Member States" include the members of ENISA's Executive and Management Board (8 members were interviewed), as well as one consulted national cybersecurity agency. "Member States" in the survey are 19 members of ENISA's Management and Executive Boards. In the context of the open public consultation, reference is made to "national authorities" which include members of ENISA's Management and Executive Boards (10 members), as well as representatives of national cybersecurity authorities (8).

Please note that ENISA's "direct stakeholders" include ENISA's Management and Executive Board representatives, members of the PSG and NLOs. The European Parliament, CERTs/CSIRTs, the Commission, other agencies and industry representatives are referred to as "(potential) users and advisors" throughout the report.

The findings of previous evaluations of ENISA's activities have shown that there is a division between the needs of Member States based on their capacity and resources invested in cybersecurity. Throughout the report, a reference is made to Member States with more experience and resources which mainly include France, Germany, the Netherlands and the UK but also cover

---

[12] Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

[13] European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

Spain, Italy and the Nordic countries to some extent. Member States with fewer resources include the Easter and Southern European Member States.

3.1 Key findings

A number of key issues emerge from the detailed findings presented below, including:

Table 10: Key findings

	• ENISA's objectives are of high relevance in the current context • ENISA's governance and organisational structure are generally conducive to an effective and efficient Agency. • ENISA has contributed to enhanced cooperation between Member States and NIS stakeholders, community building across Member States, cooperation between CERTs/CSIRTs, and capacity in Member States (notably for Member States with fewer resources for cybersecurity). It has done so through a series of activities, most noteworthy of which are the Cyber Europe Exercises. • ENISA works efficiently, implements a high number of activities and develops a large amount of publications with the resources available. • ENISA's activities are largely coherent with work at national level, notably that of Member States with fewer capacities and resources in cybersecurity, and complementary to the work of CERTs/CSIRTs.
	• ENISA lacks visibility and has not managed to become recognised as a centre of expertise or a reference point for stakeholders. • Limited resources hamper ENISA's ability to (1) respond to a wide variety of needs, (2) be effective in all areas covered by its broad mandate as it is forced to prioritise, and (3) to recruit and retain staff. • ENISA's split location in Athens and Heraklion affects its efficiency through additional travel and coordination costs. • ENISA's work programme is dominated by the interests of Member States, meaning that it does not sufficiently address the needs of other stakeholder types. Moreover, the differing needs of Member States and lack of a common line lead to work priorities representing the lowest common denominator. • ENISA lacks technical expertise, according to stakeholders, with a high reliance on external expertise over in-house expertise • ENISA had weak human resource procedures leading to difficulties in recruiting and retaining staff. • The approach to cybersecurity in the EU is not sufficiently coordinated, with few formal coordination procedures in place to ensure synergies between ENISA's activities with the policies and activities of its stakeholders; insufficiently exploited cooperation between the Commission and ENISA; and risks of overlap between ENISA and CERT-EU and between ENISA and Member States with strong cybersecurity expertise in particular.

3.2 Assessment of ENISA's performance, governance organisational structure and positioning

This section assesses the impact, effectiveness, efficiency, relevance, coherence and EU added value of the work undertaken by ENISA from 2013 to 2016 and of ENISA's governance and organisational structure. The purpose is to evaluate the implementation of the work programmes and to assess how the whole set of activities run by ENISA (including opinions, guidelines, trainings, recommendations or reports) has contributed to fulfilling its role, as described in Article 1 of the ENISA Regulation. The section presents the extent to which ENISA has become "an EU-wide centre of expertise and a reference point for EU institutions, Members States and the wider stakeholders' community, in providing guidance, advice and assistance on issues related to network and information security". Moreover, the section assesses how effectively the current governance, internal organisational structure of ENISA (Management Board, Executive Board, Executive Director and staff and PSG) and human resources policies and practices contribute to efficiencies and effectiveness in the work of the Agency. The purpose is to provide an assessment of the internal organisational structure including an evaluation of the efficiency and effectiveness of the current arrangements related to the location of ENISA's offices. This part of the evaluation also includes an assessment of how effectively the Agency sets its work priorities, as well as the degree of flexibility it has at its disposal to tackle any upcoming issues. Finally, ENISA's working relationship with the Commission, other EU institutions and bodies and stakeholders are also analysed, including the extent to which stakeholders are aware of and involved in ENISA's work.

This section relates primarily to the first dimension of this evaluation, namely the retrospective aspects. It responds to the evaluation questions, structured according to the evaluation criteria of relevance, effectiveness, efficiency, coherence and EU added value.

Please note that for each of the evaluation criteria an "overarching" question has been identified and has been responded to in the concluding section for each criterion.

3.2.1 Relevance

The evaluation criterion of relevance looks at the relationship between the needs and problems in society and the objectives of a given intervention, in this case the existence of a European agency of network and internet security.[14] The first sub-section below responds to this question by assessing the relevance of ENISA's <u>objectives</u>. As the evaluation questions presented in the Evaluation Roadmap focus on the relevance of ENISA's <u>tasks</u>, the subsequent sub-sections consider the relevance of the activities implemented by ENISA rather than its objectives.

The following evaluation questions are covered in this section:

Table 11: Evaluation questions covered under the relevance criterion

Main evaluation question	Other evaluation questions
EQ33: Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework needs?[15]	**Retrospective** EQ29: How far are the Agency's tasks and resources aligned with key EU political priorities? EQ4: How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders? EQ30: Which Agency tasks are absolutely essential to deliver on these priorities? EQ31: Which Agency tasks are necessary to continue implementing existing and

---

[14] Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

[15] For the response to this evaluation question, the use of the Agency's KPIs related to stakeholder engagement was foreseen. In the end, the data foreseen was not available (This concerns KPIs related to the uptake of the Agencies' expertise in policy documents or by industry and KPIs related to the Agencies' contribution to policy development through events).

	evolving obligations under the Treaties and EU legislative framework?
	EQ32: Are there some Agency tasks that have become redundant / negative priorities? If so, which are they?
	EQ34: Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?

3.2.1.1   Relevance of the objectives set in ENISA's mandate

EQ 33: Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework needs?
The five objectives listed in ENISA's mandate were over the period 2013-2016 and are still today of continued relevance considering the needs of ENISA's stakeholders (Member States, including CERTs/CSIRTs, the Commission and other EU institutions and the private sector) and the regulatory and policy context. The development of the cyber threat landscape over the past years shows a continued need for a response at EU level. The objective of ENISA to provide expertise is relevant as it sets the foundation for ENISA to pursue any of the other objectives. Assistance to the development of policies responds to the Commission's needs to receive sector-specific knowledge, and the assistance to the implementation of policy and legislation responds to the Commission and Member States' needs in the context of the Directive concerning measures for a high common level of security of network and information systems across the Union (hereafter NIS Directive)[16]. Strengthening Member States' capabilities and preparedness and stimulating cooperation between Member States and with private stakeholders are objectives of high relevance considering the need for combined efforts to address cyber threats across the EU.

An additional objective that ENISA's mandate could have covered is the operational support to Member States through more detailed analysis of threats and incidents to provide enhanced advice to these stakeholders.

ENISA's mandate defines five objectives for the work of the Agency[17]:
*   The Agency shall develop and maintain a high level of expertise.
*   The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security.
*   The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.
*   The Agency shall assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.
*   The Agency shall use its expertise to stimulate broad cooperation between actors from the public and private sectors.

A perceived increase in the number and variety of cyber threats over the past years, underlines the continued relevance of all of ENISA's objectives. ENISA's direct stakeholders and the other groups of stakeholders interviewed agree that with the fast pace of technological development and the increase in devices connected to the internet, the variety of cyber threats has been growing in the past years. New technologies enter the market within a few months, leading to new NIS risks. Consequently, all groups of consulted stakeholders see a continued relevance for cybersecurity efforts at EU and Member State level. The evaluations of ENISA's 2014 and 2015 core operational activities also found a clear need to address cybersecurity challenges in

---

[16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[17] Regulation (EU) No 526/2013, Article 2

the EU and the Member States. Although differences in the needs of ENISA's stakeholders were identified, the objectives of ENISA's work during 2014 and 2015 were found to be relevant to respond to the needs of Member States and stakeholders across the EU.

The objectives listed in ENISA's mandate are broadly defined. To some extent this has allowed the Agency in the past to encompass a variety of activities. Changes in the activities of ENISA based on the annual work programmes show that the way the objectives have been defined allows for flexibility to focus on different needs from one year to another. At the same time, this leads to a discontinuation of activities and limited possibilities to create strong expertise in more specific areas. ENISA's resources do not allow the Agency to fully meet its objectives (as discussed in section 3.2.3.3).

Most interviewees in the present study (including the Member States) considered ENISA's objectives to be of continued relevance. While there are differences in the objectives which are considered to be most relevant, all of them were mentioned to be very important by at least one of the stakeholder groups.

Developing and maintaining a high level of expertise is a relevant objective that lays the foundation for achieving ENISA's other objectives. The objective was considered by a majority of interviewees (including some but not all interviewees from the Member States) as a relevant objective. It was seen as the foundation for achieving ENISA's other objectives as expertise is required to understand cybersecurity threats, which is needed to prepare recommendations for the development and implementation of policies, as well as to foster cooperation between the Member States on relevant issues. Both the Member States and the Commission were described as relying on the expertise of ENISA.

In contrast, a few interviewees (including an interviewee from the Member States) noted that ENISA's objective to create and maintain a high level of expertise was not the most important one, as there is considerable expertise at Member State level. This suggests a difference between the needs of Member States depending on their capacity and the financial resources available to them in the area of cybersecurity, showing that those with less focus on this area are more dependent on ENISA's input and therefore expect the Agency to increase its expertise.

The objective to assist the Union institutions, bodies, offices and agencies in developing policies in NIS continues to be relevant as ENISA can provide added value with technical input. The objective was found to be important by all types of interviewed stakeholders. They generally saw a need for ENISA to provide technical advice to the Commission to ensure that legislation matches technical needs, for example regarding norms and standards for cybersecurity. This included interviewed Commission staff who considered the expertise that can be provided by an EU cybersecurity agency to be of high relevance to their activities. Under this objective, stakeholders expected ENISA to systematically be involved and assist the Commission when drafting legislation or policies.

The objective to provide assistance to the Union institutions, bodies, offices and agencies and the Member States in implementing policies and legislation is of particular relevance considering ENISA's role under the NIS Directive. Under the recent changes to the legislative framework, most importantly the NIS Directive, ENISA is foreseen to fulfil the function of supporting the implementation of legislation**.** The objective was mentioned comparably less often by interviewed stakeholders as one of their needs. Still, several interviewees (mainly ENISA staff and management but also representatives from other groups including the Member States) considered this objective to be relevant. ENISA's role in the context of the NIS Directive, namely to ensure its implementation, was considered very relevant by these interviewees. Industry representatives and representatives from EU institutions and bodies stated that there is a

need in the Member States for a body that ensures harmonisation and alignment of practices between the countries, as the Commission was not considered to be able to fully ensure this.

With its objective to assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to NIS problems and incidents, ENISA responds to a clear need in the Member States. The objective was considered to be of continued relevance by interviewed Member State and Commission representatives. Several Member States saw the enhancing of capabilities as a core objective, noting that there is a need for an agency to help small Member States who do not have the same capacities as larger ones. In the context of increased cyber threats, it was considered very important that the network of CERTs/CSIRTs is able to share relevant information and to consider a coordinated approach. Interviewees underlined that, to achieve this, all members of the network would need to have a certain capacity level. This underlines the relevance of ENISA's objective to enhance and strengthen capabilities and preparedness across Member States and stakeholders.

The fifth objective of ENISA, to use its expertise to stimulate broad cooperation between actors from the public and private sectors, is of continued relevance as trust needs to be built between stakeholders to ensure their cooperation on threats that often concern more than one of them at a time. The objective was considered relevant by interviewees from the Member States and the Commission. Also ENISA staff and management considered the need for enhanced cooperation to be significant. Member State respondents specifically underlined their need for cooperation between the countries to build a community with sufficient trust to ensure that exchanges of information are taking place. Members of ENISA's staff noted that the need had further developed over the past years. While initially ENISA had to convince stakeholders, in particular the Member States, that there was a need for more advanced cooperation, the Agency's objective is now to actually implement such cooperation. The need to build trust was also mentioned by respondents from the Commission who considered cooperation between the public and the private sector to be relevant to respond to current cybersecurity threats.

In summary, all present objectives were found to be of continued relevance but some stakeholders saw a need for additional objectives. Most mentioned that there was a need for operational support from ENISA. Some of the Member States saw a need to change the Agency's mandate to give it a role as an analytical centre analysing threats and incidents in detail to provide better advice to stakeholders. A few respondents (ENISA staff and Member States) also suggested that there is a need for enhanced cooperation in the field of law enforcement. The Agency could have a role in ensuring that criminal investigations on cybersecurity are more concerted and resources are pooled across the countries. As this is a role already covered by Europol, it can be assessed that changes to ENISA's mandate should be limited to suggesting further cooperation between the two agencies. Another example of an unmet need is support to private stakeholders, including small and medium sized enterprises (SMEs). A few interviewees from the private sector suggested that they could benefit from ENISA's risk assessments capacities and training on how to respond to incidents.

With regard to digital privacy issues, several interviewees noted that ENISA's objectives should remain in the area of cybersecurity as this is where the needs of the Agency's stakeholders are. During the interviews, only two respondents (European Parliament and private sector) suggested that they saw a need for ENISA to cover privacy concerns.

3.2.1.2 Alignment of ENISA's tasks and resources with key EU political priorities

EQ 29: How far are the Agency's tasks [and resources] aligned with key EU political

> **priorities?**
> ENISA's mandate and tasks are strongly aligned with key EU political priorities, most importantly the NIS Directive and the new tasks it foresees for the Agency. In general, cybersecurity is considered to be a topic of high importance and a majority of stakeholders across all spectrums considers ENISA's tasks to be well aligned with political priorities and stakeholder needs. However, Member States' needs differ and the Agency is not able to respond to all needs to the same extent.
> The adequacy of ENISA's human and financial resources is assessed under EQ16 in section 3.2.3.3.

As presented in section 1.2.1 above and in line with the Agency's objectives, ENISA's tasks can be summarised as covering the following four activities:
- Expertise provision
- Supporting the Commission in policy development
- Supporting Member States in the implementation of legislation
- Community building
- Capacity building.

ENISA's tasks are aligned with EU priorities in the area of network and information security as presented in relevant EU initiatives. NIS has been on the agenda for EU policy makers since the 2001 Communication of the European Commission on NIS[18]. The following year – the ePrivacy Directive[19] was adopted, binding providers of electronic communications services to ensure the security of their services and maintain the confidentiality of client information. Back in 2010, when the Europe 2020 strategy was adopted, a Digital Agenda for Europe (DAE) became one of the seven strategic goals for the EU future[20]. The DAE's main objective was to develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe. The third pillar of the DAE is specifically addressing Trust & Security issues[21] and serves as an umbrella for all EU conducted and coordinated activities in the field of NIS. The 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[22] sets out a strategy for the future of cybersecurity in Europe. Most recently, the NIS Directive was adopted by the European Parliament on 6 July 2016. The Directive entered into force in August 2016, giving ENISA new tasks that were not foreseen as part of its mandate, including assisting the Cooperation Group in the execution of its tasks and taking on the role of the CSIRT Network Secretariat. ENISA's tasks to foster cooperation, develop and maintain expertise in the EU, increase capacities and support the development and implementation of policy, are generally aligned with the EU priorities set out in the initiatives listed above. Moreover, the way in which ENISA's tasks are described is sufficiently broad in scope to allow for the changing EU political context to be taken into account. In particular, the new tasks foreseen for the Agency as part of the NIS Directive fall well within ENISA's current mandate – its role relative to the Cooperation Group involves assisting the Union institutions in the implementation of the policy, while its role as the Secretariat for the CSIRT Network will involve further fostering cooperation among CERTs/CSIRTs.

NIS continues to be a key political priority of the EU to which ENISA is expected to respond. In its communication of 5 July 2016[23], the European Commission encourages Member States to make the most of NIS coordination mechanisms. According to the NIS Directive, ENISA

---

[18] COM(2001)298, Network and Information Security : proposal for a European Policy approach

[19] Directive 2009/136/EC Of The European Parliament And Of The Council Of 25 November 2009

[20] COM (2010) 2020 final, Communication From The Commission Europe 2020. A strategy for smart, sustainable and inclusive growth; Brussels, 3.3.2010

[21] Digital Agenda for Europe, Pillar III: Trust &Security <https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security>

[22] COM (2016)410, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

[23] European Commission , *Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threat*s, Press release, Brussels, 5 July 2016

will have a stronger role to support this coordination. Stakeholders across all interviewed groups agreed that NIS was one of the key EU political priorities, mainly considering the increasing frequency, variety and intensity of cyber threats and suggested that ENISA should be part of the response to these.

Overall, ENISA's tasks are considered to be well aligned with the priorities of its stakeholders. This was noted by a majority of interview respondents, in particular ENISA's direct stakeholders. They highlighted ENISA's work on ensuring interaction and exchange between the Member States, increasing capacity in the Member States and raising awareness of cybersecurity issues. With regard to specific tasks, ENISA's expected work under the NIS Directive was highlighted as an example of where ENISA's tasks are particularly well aligned with the political priorities. Exercises and the Threat Landscape reports[24] are examples of where ENISA is meeting the needs of its stakeholders.

Satisfaction with ENISA's activities can also be seen in the responses to the survey of CERTs and CSIRTs as presented in Figure 6 below. Survey respondents were in most part satisfied with the extent to which ENISA covered the needs of CERTs/CSIRTs over the 2013-2016 period. A large majority of respondents (28 out of 34) thought ENISA covered the needs of CERTs/CSIRTs to a high or to some extent during that period, while six out of 34 thought it did so to a limited extent.

Figure 6: To what extent did ENISA cover CERTs/CSIRTs' needs over the 2013-2016 period?
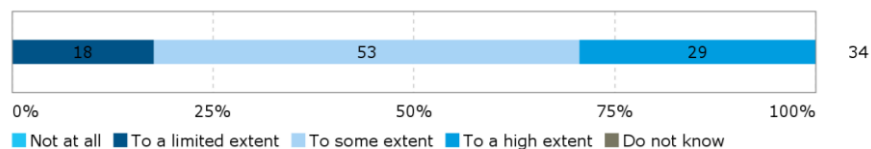
Source: CERTs/CSIRTs survey

Stakeholders suggest that ENISA's tasks respond to the key policy priorities due to the strong influence of the Member States on the mandate. The 2014[25] and 2015[26] annual evaluations of ENISA showed that ENISA's activities during these years were clearly linked to the Agency's legal mandate. There were no cases falling outside the scope of the mandate. Interviewees in the present study (Member States, ENISA staff and EU institutions and bodies) mentioned the delivery of tasks according to its mandate as one of the reasons why ENISA's work is well aligned with political priorities. As the work programme itself is set by the Commission and the Member States, it is aligned to their intentions and needs. ENISA staff and management suggested that they were well prepared to respond to changing priorities and the needs of the Agency's constituency.

There are differences with regard to stakeholders' needs in the context of the key EU political priorities. Between the Member States there is disagreement on the extent to which ENISA should cover specific topics, such as certification[27] or whether ENISA should develop operational capacities which could include responsibilities in the area of detection and response to cybersecurity threats. While some Member States would welcome ENISA's support in this area, others have developed their own capacities. In general, Member States with less capacity and fewer resources in the cybersecurity area (e.g. Eastern and Southern European countries) tend to be in favour of further support by ENISA while Member States with more resources and experience

---

[24] ENISA publishes every year a report summarising the most prevalent cyber-threats, entitled Threat Landscape

[25] Ramboll Management Consulting (2015) External Evaluation Of ENISA, focussing on ENISA's 2014 activities.

[26] Ramboll Management Consulting (2016) External Evaluation Of ENISA, focussing on ENISA's 2015 activities. Ramboll Management Consulting (2015) External Evaluation of ENISA, focussing on ENISA's 2014 activities.

[27] "Certification" means the implementation of common security certification frameworks for Information and Communication Technologies against harmonized principles a/o standards. Many stakeholders see a role for ENISA in the development of these standards and the application of a certification scheme for the public and/or private sector.

(e.g. Germany, France, the Netherlands and Sweden) do not see the necessity for ENISA to cover these issues.

3.2.1.3   Balance between cybersecurity and digital privacy topics

> **EQ4: How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders?**
> When only considering the identified needs of ENISA's main stakeholders, the Agency should focus on the cybersecurity area and disregard digital privacy topics. However, the evaluation identified some potential benefits of giving responsibilities to ENISA to ensure greater coordination between the cybersecurity and digital privacy areas.

In the preamble to the Regulation, the objectives linked to cybersecurity and digital privacy topics are presented on an equal footing ("*The Agency should contribute to a high level of network and information security, to better protection of privacy and personal data…*"). However, protection of privacy and personal data are not listed among the objectives listed in the Regulation itself. This leaves room for some discussion on the extent to which ENISA should respond to privacy issues and how these activities should be balanced with the cybersecurity tasks it performs. This fact is also reflected in stakeholders' feedback on this issue.

The main needs of ENISA's stakeholders lie in the area of cybersecurity; digital privacy topics are not considered to be a priority. A number of interviewees (mainly from EU institutions and bodies) noted that they were not aware of any activities of ENISA in the area of privacy protection but also did not consider this to be a relevant issue in its work. Furthermore, most of ENISA's direct stakeholders explicitly stated that ENISA should not be covering digital privacy topics, arguing that the Agency should focus its limited resources on cybersecurity topics and that there were other bodies which were better equipped to cover the privacy area such as the European Parliament, DG JRC or the European Data Protection Supervisor (EDPS).

Stakeholders saw potential benefits for ENISA, its stakeholders and society at large if the Agency were to act as a broker, supporting cooperation across the digital privacy and cybersecurity issues. Several interviewees from the group of users and advisors pointed to intersections between cybersecurity (e.g. the security of electronic communication) and digital privacy. In these areas ENISA could provide its expertise and share solutions that relate to security and privacy at the same time. One of the interviewees suggested that in the Member States there was a gap between cybersecurity and data protection, suggesting that national representatives working in these two areas would not necessarily be cooperating in all Member States and that ENISA could be the one to start such cooperation.

3.2.1.4   Essential tasks to deliver on key EU political priorities

> **EQ30: Which Agency tasks are absolutely essential to deliver on these priorities?**
> Among the four tasks of ENISA (capacity building, expertise, community building and policy implementation and development), community building stands out as being absolutely essential. ENISA's stakeholders considered the Agency to be best placed to foster cooperation across the Member States and with other stakeholders.

Different groups of stakeholders see different priorities for ENISA which makes it difficult to rank ENISA's tasks according to their relevance. In particular ENISA's direct stakeholders and the representatives of national CERTs/CSIRTs consider capacity building to be

essential. They underlined the need to ensure that Member States grow their expertise based on ENISA's support. Specifically the cyber exercises[28] were mentioned as a highly relevant activity.

Among EU-level institutions and other stakeholders, such as industry, community building and the provision of expertise were considered to be essential. With tasks covering <u>expertise</u>, ENISA is expected to anticipate and support the EU as a whole in facing emerging NIS challenges by making information on cybersecurity available and accessible to the EU. Stock taking of practices and experiences across the EU and best practices disseminated to Member States and the industry were considered to be of high relevance. Several Commission DGs highlighted the capability of ENISA to provide thematic expertise in their relevant sectors.

ENISA's work to establish and facilitate dialogue between the Member States' authorities and with industry stakeholders and academics is considered essential. This work of <u>community building</u> is expected to foster collaboration allowing Member States to better respond to cyber threats.

Finally, across the different stakeholder groups, some interviewees suggested that ENISA's <u>policy</u> work was essential. These stakeholders suggested that ENISA had a key role in supporting policy implementation. Some also mentioned that they expected ENISA to provide input to policy development based on their expertise, but saw a need for the Agency to improve the dissemination of their knowledge and their visibility to take on this role.

The key current demands or needs according to the different types of stakeholders are summarised in Table 12 below.

Table 12: Key current demands or needs according to the different types of stakeholders

Stakeholder type	Key demands for ENISA
European Commission	Community building Expertise provision Supporting policy development / implementation
Member States with strong capacities and more resources	Community building Supporting policy development at EU level
Member States with fewer resources and capacities	Capacity building Supporting policy development at EU level Supporting policy implementation at national level Community building Expertise provision
CERTs/CSIRTs	Capacity building
Industry	Community building Expertise provision Supporting policy development / implementation

Among the four tasks, the one that stands out as most essential is that concerning community building. When interviewees were asked what the consequences of a discontinuation of ENISA would be (see section 3.2.5.3), respondents across all stakeholder groups saw a huge need for continuation of cooperation across the Member States (in particular between the CERTs/CSIRTs) and also with other stakeholders and considered ENISA as best placed to ensure this.

3.2.1.5   Necessary tasks to implement existing and evolving obligations

EQ31: Which Agency tasks are necessary to continue implementing existing [and evolving] obligations under the Treaties and EU legislative framework?
The evaluation findings show that different specific activities within ENISA's four tasks (capacity, expertise, community and policy) are considered necessary to continue responding to the Agency's

---

[28] ENISA leads a wide range of activities in the field of cyber exercises. They are related with to activities on increasing capacities in cyber crisis management. Most mentioned were the Cyber Europe Exercises.

existing and evolving obligations. ENISA's obligations under the EU legislative framework can cover a wide array of tasks which respond to stakeholders' current needs. Some suggestions of services that could have been provided by ENISA were made (including the provision of real-time cybersecurity information and further guidelines and benchmarks for the public and the private sector), but stakeholders would not be willing to pay for additional products or services.

Evolving obligations under the Treaties and the EU legislative framework are discussed in sections 3.3.1 and 3.3.2.

ENISA's obligations under the Treaties and the EU legislative framework cover a broad area and primarily depend on what the Member States are expecting from ENISA and what is included in the Agency's annual work programmes. ENISA's direct stakeholders describe the Agency's existing obligations as stemming from its unique position as a neutral player in the field of cybersecurity, serving Member States and the EU institutions. According to these stakeholders, ENISA's obligations include an objective to ensure harmonisation across the Member States to align their cybersecurity capabilities and capacities. Furthermore, they mention specific legislation requiring ENISA's attention, such as the NIS Directive and the General Data Protection Regulation[29]. ENISA's obligations based on Regulation (EU) No 526/2013 are perceived as being broad and rather flexible, requiring the Member States to define what they are expecting from the Agency.

Across the four main tasks of the Agency, there are a number of specific activities that are considered to be relevant by stakeholders. Among the respondents to the open public consultation, the products and services most frequently listed as being "relevant" or "very relevant" to respondents' work or activities were reports and research publications (82% or 51 out of 62 respondents), guidelines and recommendations, including publications on standards (81% or 50 respondents) and events (65% or 40 respondents). In contrast, 48% of respondents (30) indicated that Article 14 requests were not at all relevant to their work or activities. These requests can however only be used by Member States and the Commission. Respondents from national authorities considered most often selected guidelines and recommendations (9 out of 15), reports and research publications (6 out of 15), and the Cyber Europe Exercise (8 out of 15) as "very relevant". Article 14 requests were considered to be "not relevant" by five national authority respondents.

---

[29] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Figure 7: Relevance of products/services to respondents' work/activities (n=62)

	Very relevant	Relevant	Somewhat relevant	Not relevant
Guidelines & recommendations, including on standards	24	26	12	
Training or workshop opportunities	12	21	18	11
Training material or toolkit	8	17	21	16
Reports (e.g. NIS Threat landscape) and research publications	24	27	10	1
The Cyber Europe Exercise	18	16	14	14
Technical advice, including support to policy development and or implementation	12	14	20	16
Events	13	27	19	3
Article 14 requests	9	10	13	30
Other	1		9	

Source: Open public consultation

In the context of the open public consultation, respondents were asked if there were any other products or services they would have liked ENISA to provide the cybersecurity community with over 2013-2016. Out of 62 respondents, 65% (40) answered "no", while 35% of respondents (22) answered "yes" which were primarily constituted of private enterprise or business association respondents. Only two respondents from national authorities responded "yes" to the question. These respondents were asked to further specify what kind of services they would have liked ENISA to provide. Their responses can be categorised into three broad topic areas, namely: operational capacities, cross-country cooperation (across Member States and with non-EU countries) and the provision of policy advice and guidelines. With regard to products and/or services related to ENISA's operational capacities, respondents would have liked ENISA to provide near real-time cybersecurity warnings and consider developing a panel of security operation services to address cross-country cyber incidents. With regard to products and/ or services related to cooperation across Member States, respondents would have liked ENISA to encourage information sharing to support the adoption of new regulations and incident handling procedures as well as supporting cybersecurity capacity building. Respondents would have also liked ENISA to make visible the kind of expertise and knowledge available in Member States. With regard to products and/or services related to cooperation with stakeholders outside the EU, respondents would have liked ENISA to work together with the public and private sector to act as a contact point for cybersecurity organisations from outside the EU allowing it to also promote European security technology in foreign markets and provide cybersecurity capacity building in third countries. Finally, with regard to products and/or services related to policy and guidelines, respondents would have liked ENISA to provide benchmarks and best practices to help establish the framework for an EU cybersecurity strategy. These could cover for example, cybersecurity priorities for research and development and securing critical infrastructure. It was also suggested that ENISA could contribute by creating horizontal policy documents and guidelines across for exchange across EU bodies.

Open public consultation respondents were further asked whether they would be willing to pay for additional services if they were provided by ENISA. Only 14% of respondents (3) who would have liked ENISA to provide further services over the 2013-2016 period indicated they would be willing to pay a fee in the future for the additional products or services they would have liked ENISA to offer during 2013-2016.

Figure 8: Respondents willing to pay a fee to obtain additional products/services from ENISA over 2013-2016? (n=22)
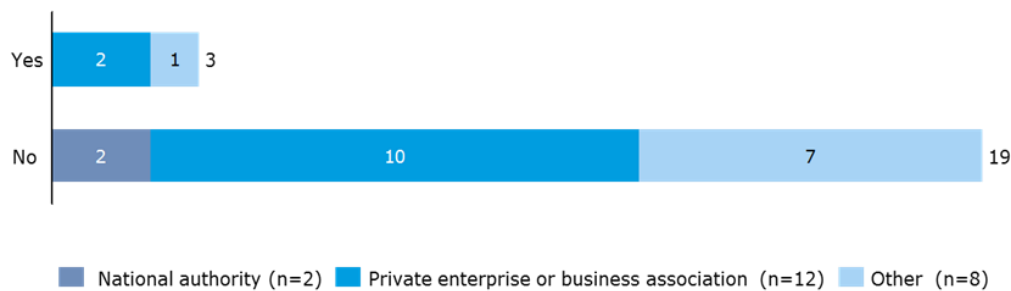
Source: Open public consultation

3.2.1.6   Tasks that potentially have become redundant

EQ32: Are there some Agency tasks that have become redundant / negative priorities? If so, which are they?
The evaluation has not identified any redundant tasks implemented by ENISA. The assessment of the relevance of ENISA's tasks strongly depends on stakeholders' differing needs. The Management Board seems to set the right priorities, though some stakeholders would like ENISA to be able to act more on their own initiative.

Based on the stakeholder consultation, no tasks of ENISA have been identified as being redundant or a negative priority. Interviewees across all groups stated that there was no redundant work done by ENISA. In particular in the context of a very restricted budget, ENISA would ensure that only relevant tasks were being implemented. The Management Board was mentioned as an important mechanism to ensure the relevance of all of ENISA's tasks. Similarly, from the open public consultation, no task or activity of ENISA emerged as being potentially redundant.

The only activity that was mentioned by more than one interviewee as something ENISA should not focus on was the work in the area of privacy which two interviewed stakeholders considered to be outside the Agency's key competences. Other responses to the question on redundant tasks, on the one hand, showed that needs differ between the Member States based on their national capacity and resources. Interviewees mainly referred to tasks that could be made more relevant by implementing some improvements rather than suggesting that these tasks be completely abandoned. Although no redundant tasks were identified, some interviewees suggested that ENISA should be able to act more on its own initiative and could intervene more strongly to set priorities when the members of the Management Board have opposing opinions or when suggested tasks only respond to Member States' needs and leave out those of other stakeholders.

3.2.1.7   Non-core activities becoming part of the core-business

EQ34: Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?
There are activities which have moved from non-core to the core-business of the Agency, such as specific training activities or the topic of critical infrastructures. These changes can be assigned to technological developments and changes in the needs of the Member States based on legislation, their capacities and preferences.

Over time, some of ENISA's activities have moved from non-core to being part of the core-business, but the development can also be noted in the opposite direction. ENISA's direct stakeholders and ENISA staff mentioned examples of changes in ENISA's core activities,

such as in the area of capacity building and training. These were initially key tasks of the Agency which became less of a focus with growing levels of expertise in certain Member States, but more recently have become a priority once again with the implementation of the NIS Directive. Another example provided relates to critical infrastructures which Member States with strong cybersecurity expertise initially preferred covering themselves, but more recently they have welcomed ENISA's support in this area. According to ENISA staff, awareness raising has been less prioritised over the years, mostly as Member States have taken on part of the activities themselves, for example in the planning and implementation of the Cybersecurity Month.

The priorities set among the Agency's tasks depend on the demand from the Member States and the technological evolution. With ENISA's broad mandate it is possible to change priorities with regard to specific tasks from one year to another. The priorities set depend on the one hand on technical developments which require ENISA to set their focus on a specific area, such as with the evolution of the Internet of Things (IoT). On the other hand, the Member States can, through their position in the Management Board, decide what ENISA should be focussing on (see section 3.2.2.5 for more information of ENISA's effectiveness at setting its work priorities). Where ENISA helps them to put in place a specific initiative, the Member States might be able to implement the work themselves after some time. With changing legislation, the Member States might require support from ENISA in a new area.

3.2.1.8   Conclusion on relevance

Conclusion – Relevance

The baseline situation (established based on an evaluation of all EU agencies including ENISA in 2009[30] and an impact assessment of changes to ENISA's mandate in 2010[31]) shows an increasing dependence on NIS across ENISA's stakeholders and increasing expectations on what the Agency should be delivering. The impact assessment of 2010 concluded that the tasks listed in the Regulation on ENISA were insufficient to provide the Agency with the necessary flexibility and adaptability to respond to the continuously evolving NIS environment.

The assessment of ENISA's relevance over the period 2013-2016 concludes on the continued relevance of NIS. It points to the fact that ENISA has a broad mandate which allows it to take on new topics as they emerge. However, at the same time, the Agency has difficulties meeting all of its objectives resulting from its broad mandate due to limited resources; it is often forced to prioritise (see section 3.2.2).

In the context of technological developments and evolving threats, over the period 2013-2016 there was a significant need for increased NIS in the EU. This continues to be the case today. The recent additions to the legislative framework, such as the NIS Directive and the Commission's communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry[32] underline this. Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. Based on its mandate, ENISA is intended to respond to these needs.

Considering this context, the objectives set out in ENISA's mandate continue to be of high

---

[30] Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

[31] European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

[32] European Commission: Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry COM(2016) 410 final

relevance today.

These objectives also leave room for ENISA's Management Board to set priorities based on latest developments in order to respond to changing needs and evolving threats.

While ENISA's mandate remains relevant, its activities do not fully meet the needs of all t stakeholders for two main reasons:

- ENISA relies on its the Member States and the European Commission to provide clear guidance via the Management Board on where its contribution is most needed. Its work programme is dominated by the interests of Member States, and yet it is necessary to consider the longer-term perspective and the activities of other stakeholders in the cybersecurity area (such as other EU agencies) to ensure continued relevance of the Agency.
- ENISA's stakeholders strongly differ in their needs, making it difficult to meet them all. Some Member States (such as Germany, France or Sweden) have significant capacity and resources in the area of cybersecurity and rely on ENISA only for specific services. Other Member States (from Eastern and Southern Europe) are less experienced and rely more strongly on the expertise and capacity of ENISA. The Commission has their own needs and expectations with regard to the services that ENISA can provide the different DGs with. Additionally, industry stakeholders, including a high number of SMEs are important actors in NIS and could also benefit from ENISA's activities.

ENISA could respond better to stakeholders' needs by providing operational support to Member States through analysis of threats and incidents to provide enhanced advice to these stakeholders and support response cooperation.

Among ENISA's direct stakeholders, cybersecurity needs prevail over digital privacy needs.

3.2.2 Effectiveness

This section covers the evaluation criteria effectiveness. The effectiveness analysis considers how successful EU action, in this case the activities of ENISA, have been in achieving or progressing towards its objectives[33]. It also includes an assessment of the effectiveness of ENISA's governance and internal organisational structure.

The following evaluation questions are covered in this section:

---

[33] Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

Table 13: Evaluation questions covered under the effectiveness criterion

Main evaluation question	Other evaluation questions
EQ1 To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate?	**Retrospective** EQ2: What have been the benefits of acting at agency level both from the operational and strategic perspective? EQ3: To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe? What more could be done? EQ5: To what extent has ENISA become an EU-wide centre of expertise and a reference point for stakeholders[34] in providing guidance, advice and assistance on issues related to network and information security? EQ6: How effectively has the Agency managed to set its work priorities? EQ7: How effectively does the Agency tackle important upcoming, unplanned issues deriving by demands of its constituencies and/or EU policy priorities? EQ8: Does the Agency consistently perform the same tasks with the same quality level over time? EQ11: How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to effectiveness in the work of the agency? EQ12: How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate? EQ13: What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives? EQ19: To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc.)? EQ20: To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?

3.2.2.1   Implementation of tasks and achievement of objectives

EQ1 To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate?

ENISA successfully implements the tasks set by its annual work programmes and achieves targeted KIIs. However, ENISA has difficulties covering the entire spectrum of the broad mandate in each of the work programmes due to limited resources. Consequently, ENISA makes a more significant contribution to some of its objectives, in particular enhancing cooperation and ensuring capacity building in the Member States. The objectives to develop and maintain expertise and to support the development and implementation of policy are attained to a smaller extent. The activities of the Agency that benefit the private sector directly are limited. The Cyber Europe Exercises, support to CERTs/CSIRTs, its publications and the Cybersecurity month are some of ENISA's main achievements.

There is a generally positive, but not excellent, perception of ENISA's work over the period 2013-2016. Respondents to the open public consultation were asked to give an overall assessment of ENISA for the period. Overall, 74% of respondents to the open public consultation (48 out of 65) had a positive (very good or good) view of ENISA. The overall assessment of ENISA

---

[34] The stakeholders include EU institutions, Members States and the wider stakeholders community

was more positive among national authorities, while respondents from the private sector were more likely to indicate their overall assessment as being "fair".

Figure 9: Overall assessment of ENISA for the period 2013-2016, (n=65)
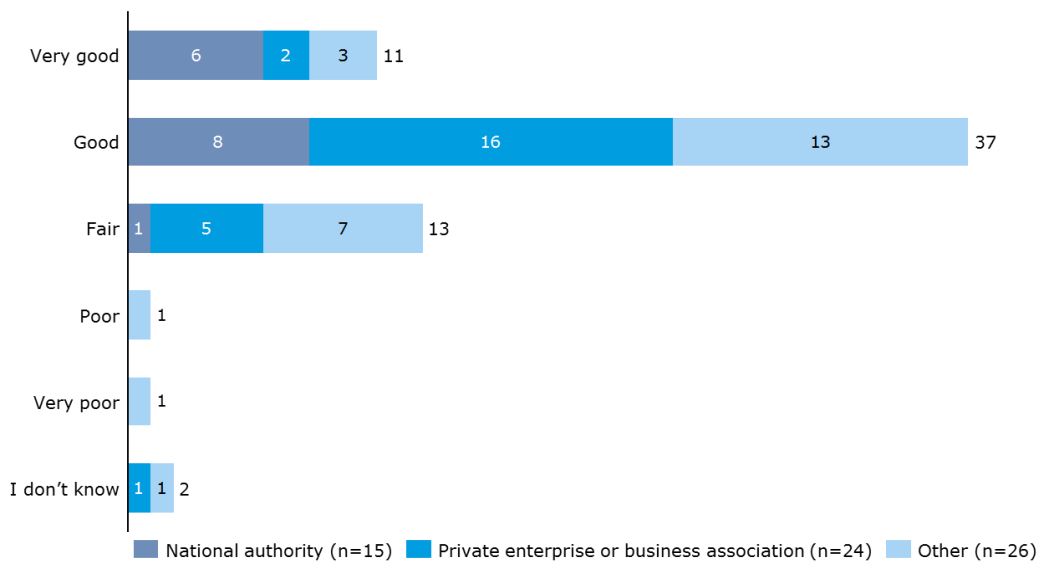
Source: Open public consultation

ENISA attempts to implement all its tasks. For some of the activities, there is mixed feedback on their degree of quality. Based on its mandate and the annual work programmes, ENISA implements the tasks assigned to it. The main outputs of the Agency's activities are publications as presented in Table 14 below. Reports are available for download on ENISA's website and statistics of downloads show that downloads of publications have been consistently high over the four years under review.[35]

Table 14: Achieved outputs[36]

	2013	2014	2015	2016
Number of publications	54	45	52	64
Number of downloads	856,017	766,385	808,923	901,464
Number of training sessions	not available	11	10	11
Number of participants per training	not available	190	170	150
Number of exercises	1	1	1	2
Number of participants per exercise	30-50	600-800	40-50	900-1100

Source: information provided by ENISA

ENISA's training sessions are targeted at CERTs/CSIRTs. In 2015, CERTs/CSIRTs from seven Member States received training, involving various private and public organisations.[37]

Feedback on the quality of the Agency's outputs is varied. A number of interviewees from all stakeholder groups suggested that the degree of usefulness and quality of ENISA's reports/publications was not always satisfactory. Feedback on trainings from CERTs/CSIRTs

---

[35] An assessment of further outputs has not been made as output indicators change from one year to the next and thus do not allow to make comparisons over the years.

[36] This data was provided by ENISA.

[37] ENISA (2016): Activity report 2015

received during interviews and the workshop was generally positive, while the views on the Cyber Europe exercises were more mixed. Some stakeholders considered their participation in the exercises to be beneficial, whereas others were concerned about the high number of participants making the exercises more complex and slower. The quality of ENISA's outputs is further discussed in section 3.2.2.7.

ENISA generally achieves short term KIIs but it is more difficult to establish its contribution to long term objectives. ENISA sets KIIs for the monitoring of the implementation of the work programmes. In general, these have been achieved according to the annual reports in 2013, 2014 and 2015. Only for a few long term targets set for 2015 the annual report of that year noted that it was too early to judge the degree of achievement. The annual evaluation of 2015 stated that there is a clear pattern in terms of progress, where targets under ENISA's control (such a high quality, community building, good practice dissemination) are largely achieved. The progress towards more long term objectives looks more uncertain (preparedness to respond to crisis, increase in capacity etc.), as this is highly dependent on contextual factors as well as public and private stakeholders' engagement and investment. Still, ENISA does achieve some of its targeted objectives and the large majority of stakeholders agree that ENISA makes a contribution to increased NIS across Europe.

ENISA achieves its objectives but to varying degrees across the different activities. All respondents to the open public consultation indicated that ENISA had achieved at least some of its targeted objectives to some extent or to a great extent. Respondents were asked to evaluate the extent to which they felt ENISA had achieved the objectives set out in its mandate during the period of 2013-2016. The assessment made by 65 respondents is presented in Figure 10 below. The objective of "developing and maintaining a high level of expertise in cybersecurity" was selected as being achieved to a great extent or to some extent by the highest number of respondents (86% or 56 respondents), followed by "supporting cooperation in the cybersecurity community, e.g. through public-private cooperation, information sharing, enhancing community building, coordinating the Cyber Europe Exercise" (79% or 51 respondents). "Supporting the implementation of EU policy" was selected by all of the respondents from national authorities as being achieved either to some or to a high extent. National authorities generally indicated that ENISA had achieved all its objectives "to some" or "to a large extent" with few respondents selecting "to a limited extent" (3 out of 15 for "supporting the development of EU policy" and 4 out of 15 for "supporting Member states to strengthen their capacity and preparedness").

Figure 10: Extent to which ENISA has achieved its objectives over 2013-2016, (n=65)
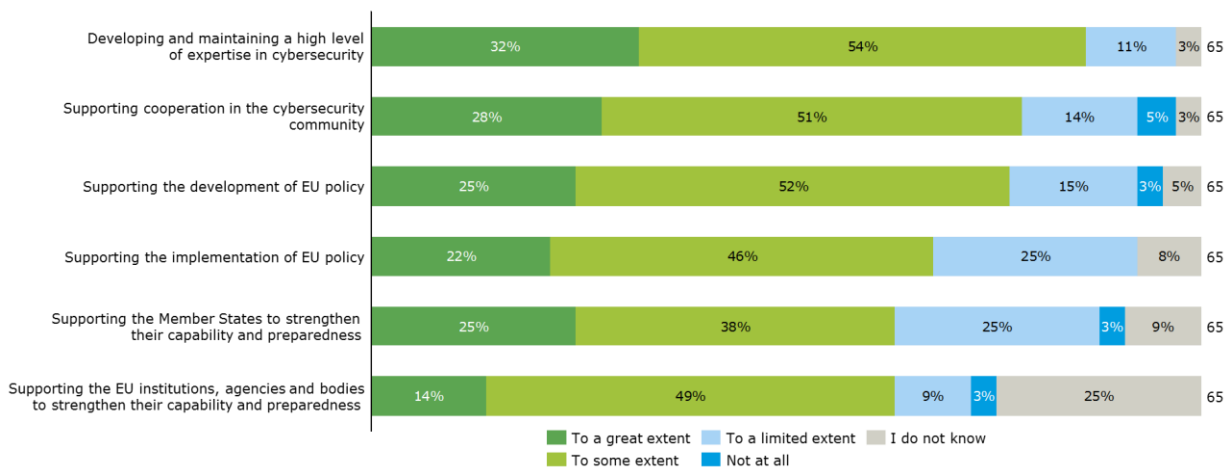
Source: Open public consultation

All respondents to the open public consultation were asked to list what they thought were the main achievements of ENISA over the 2013-2016 period. In total, 55 responses were received. The following points were mentioned by several respondents:

- The coordination of the Cyber Europe Exercise
- The provision of support to CERTs/CSIRTs through training and workshops fostering coordination and exchange.
- ENISA's publications (guidelines and recommendations, threat landscape reports, strategies for incident reporting and crisis management etc.) that were considered as useful to create and update national security frameworks, as well as for reference to policy makers and cyber practitioners.
- Assisting with the promotion of the NIS Directive
- Efforts to increase awareness on cybersecurity via the cybersecurity month.

National authority respondents believed another main achievement was the support ENISA provided to Member States in particular fostering cooperation by sharing of expertise among Member States, information sharing on Art. 13, and support for the implementation of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[38]. Private enterprises and business associations also commended ENISA's work in fostering public-private cooperation and increasing better cross-sector engagement, providing a degree of "coordination and harmonisation that might have otherwise been missing". They also felt that another main achievement was that ENISA had established itself as a "relevant, neutral reference point of cyber expertise in Europe with demonstrated EU added value". As well as being a source of knowledge that is easily accessible and easy to use covering a wide range of cybersecurity topics.

As concluded in the evaluations of the Agency's activities, ENISA´s 2014 and 2015 activities have made important contributions to enhancing cooperation both between Member States of the EU and between related NIS stakeholders. The assessment was made based on survey findings which pointed to the fact that the support from ENISA has contributed to a great extent to enhancing community building in Europe and beyond, increased cooperation of operational communities and improved workflow and communication among stakeholders. Interview results supported these findings, with stakeholders stressing the positive role that ENISA has in bringing people together to discus and cooperation.[39] In extension of this finding, it is assessed that ENISA has contributed to a great extent to enhancing community building in Europe and beyond.

ENISA´s activities contributed to some extent to capacity building, and to varying degrees depending on the stakeholder type. In this regard, the evaluation of ENISA's 2015 activities finds that ENISA's support has allowed for the development of sound and implementable strategies to ensure preparedness, response and recovery in the Member States and contributed to developing capacities in prevention, detection, analysis and response at national level. The findings further suggest that ENISA has assisted in enhancing the capacity of Member States (most notably Member States with fewer resources and capacities) in particular through: the pivotal role it plays in bringing different actors together and building networks; the dissemination of good practices; and the organisation of training sessions (e.g. for CERTs/CSIRTs) on a technical level. The evaluation concluded that the support provided by ENISA was perceived as complementary to that of other public interventions, clearly pointing to a role for ENISA in relation to capacity building.[40] The contribution to capacities of the private sector of ENISA's activities is more uncertain according to the annual evaluations and the interviews conducted in the context of the present evaluation. The 2015 evaluation of ENISA's activities concluded that there was still a long road

---

[38] Regulation –(EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[39] Ramboll (2016): External evaluation of ENISA – 2015, Final report
[40] Ramboll (2016): External evaluation of ENISA – 2015, Final report

ahead before an EU-level crisis management process was put in place in the cybersecurity area mainly due to a lack of trust among stakeholders, weaknesses and differences in national capabilities and insufficient exchanges of information in "real life". This conclusion was also reflected in the interviews for the present evaluation.

ENISA's contribution to the <u>development and maintenance of a high level of expertise</u> of EU actors is limited. On the one hand, evidence from the previous evaluations and the interviews confirm that ENISA´s activities do provide some stakeholders (e.g. critical information infrastructures (CIIs), CERTs/CSRITs) with advice and assistance. On the other hand, evidence suggests that these activities have not contributed as significantly as intended towards the adoption of methods towards new technologies and enabling the exploitation of the opportunities in emerging technologies.

The contribution towards <u>implementing and developing policies</u> was considered to be the least achieved objective by the interviewed stakeholders. While efforts have been made to prepare for the implementation of the NIS Directive, the Agency is not consistently being involved in all NIS related activities of the Commission. Interviewees from the different Commission DGs indicated that ENISA could be more involved in their process of developing policies. In turn, ENISA's staff and management noted that they were not always fully aware of all Commission activities related to cybersecurity, most notably considering initiatives of DGs other than DG CNECT.

Obstacles to achieving the targeted objectives stem from a broad mandate. When assessing the achievements of the Agency, it becomes clear that a lot of efforts are being made but they are spread over a wide field of responsibility. The fact that cybersecurity is such a broad topic and that ENISA's stakeholder community is so diverse compounds the issue.

Within the NIS community there is a wide spectrum of expectations towards ENISA across the various stakeholders but with the limited resources at its disposal, ENISA has to set priorities. This means that the Agency is not able to implement all tasks set out in the mandate to the same extent. In the development of the annual work programmes some tasks are prioritised over others. Generally, ENISA implements all the tasks set out in the annual work programmes.

3.2.2.2   Benefits of acting at agency level

EQ2: What have been the benefits of acting at agency level both from the operational and strategic perspective?
ENISA has filled a gap by acting as a neutral, independent broker at EU level. It has helped to bring stakeholders of various types and from various sectors together and acted as a bridge between the strategic and operational worlds, thereby contributing to its ultimate goal of increasing network and information security in Europe. That being said, its work programme is heavily influenced by Member State interests and there is scope to increase the Agency's impact.

Acting at agency level provides for independence and neutrality. A number of interviewees across all groups stressed the neutral position of ENISA as an Agency as one of its key strengths – it was seen as providing advice that is not influenced by industry or political interests. This was particularly appreciated by respondents to the open public consultation from private enterprises and business associations, noting that having established itself as a "relevant, neutral point of cyber expertise in Europe" was one of ENISA's main achievements. The findings of the 2015 evaluation also supported this with the case studies conducted confirming that ENISA´s activities in 2015 were generally relevant to both the public and private sector on national level, in particular since ENISA is an important neutral source of information, in a field where many reports would be written, for example, by providers themselves wanting to sell their own solutions.

ENISA has acted as a bridge between the strategic and operational worlds. From an operational perspective, ENISA managed to cover the needs of national CERTs/CSIRTS. A large majority of respondents to the CERT/CSIRT survey (28 out of 34) thought that ENISA covered the needs of CERTs/CSIRTs to a high or to some extent during the 2013-2016 period.

Figure 11: Extent to which ENISA covered CERTs/CSIRTs' needs over the 2013-2016 period
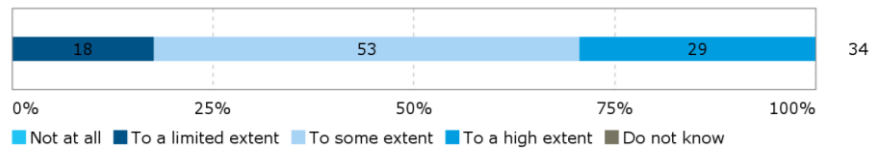
Source: CERT/CSIRT survey

From a strategic perspective, ENISA is considered important in its ability to bridge the policy/operational divide through the provision of policy support and the creation of a network of stakeholders from various organisations and sectors. Interviewees from different stakeholder groups perceived the NIS Directive as an opportunity for ENISA to expand this role.

As an Agency governed by a Management Board made up primarily of Member States, ENISA's work priorities are heavily influenced by the interests of Member States. Interviewees from the group "users and advisors" and ENISA staff pointed to the fact that Member States were key in determining ENISA's work priorities, sometimes at the expense of the needs and interests of e.g. industry, certain types of Member States (see section 3.2.2.5).

3.2.2.3   Contribution to increasing network and information security in Europe

> **EQ3: To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe? What more could be done?**
> The evaluation finds that ENISA has clearly contributed to increasing network and information security in Europe through its various activities and their outputs and results. However, the Agency is limited in its contribution to this goal due to its mandate, its resources and a lack of visibility. A number of suggestions were made on how ENISA could further contribute to NIS in Europe, however these rely on additional resources being at its disposal.

According to the intervention logic (presented in Appendix 1) based on Regulation (EU) No 526/2013, ENISA's work is intended to contribute to a high level of network and information security. The Regulation understands network and information security as "*the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems*" (Article 1.3).

ENISA has made a clear contribution to the overall goal of increasing network and information security in Europe. As presented in section 3.2.2.1, ENISA has generally been successful in the implementation of its tasks and the achievement of the KIIs set by the Management Board. The two previous evaluations showed that ENISA clearly contributes to ensuring a high level of NIS in the EU (including by sharing good practices in NIS, as shown in the stakeholder survey carried out by the 2015 evaluation), which should be seen as a strong achievement. A survey conducted among members of ENISA's Management Board, NLOs, the PSG and a small sample of industry stakeholders in the context of the 2014 evaluation, found that 74% of respondents (42 out of 58) agreed or strongly agreed that ENISA contributed to ensuring a high level of NIS within the EU. A strong majority of interviewees in the present study also agreed that ENISA contributed to this overall goal. A number of activities were mentioned through which this

contribution was made, including ENISA's work on developing networks, the exercises and training activities, awareness raising activities and the provision of the Agency's expertise.

A more concrete example of the impact of ENISA's work can be found in the survey of CERTs/CSIRTs, in which respondents were asked about the importance of ENISA's capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) in 2013-2016. Respondents were very positive as to its importance for CERTs/CSIRTs' development. As can be seen in Figure 12 below, almost all respondents (33 out of 34) thought that such capacity building activities were either very important or important.

Figure 12: Importance of ENISA's capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) in 2013-2016 for CERTs/CSIRTs' development
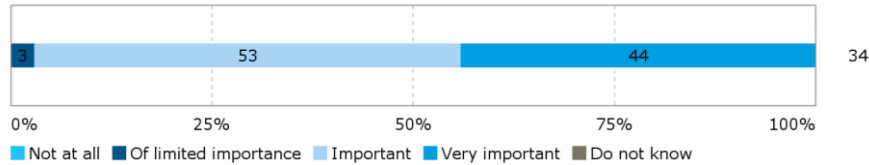
Source: CERT/CSRIT survey

There are limits to what ENISA can achieve with regard to increasing NIS in Europe. Stakeholders mentioned limitations to the Agency's effectiveness. These include a lack of visibility, making it difficult to reach the targeted stakeholders with their publications and expertise, and a general underestimation of the relevance of cybersecurity issues by different stakeholders across the EU.

A number of interviewees from the group of "users and advisors" noted that they would not be able to respond to questions regarding ENISA's impact. This suggests that there is limited visibility of ENISA's successes.

3.2.2.4   EU-wide centre of expertise and reference point for stakeholders

EQ5: To what extent has ENISA become an EU-wide centre of expertise and a reference point for stakeholders in providing guidance, advice and assistance on issues related to network and information security?
With the exception of very few stakeholders, ENISA was not described as a centre of expertise or as a reference point for stakeholders in the NIS area. The Agency is more considered as a valuable partner for ensuring coordination across the EU. Its guidelines and reports are used by many stakeholders, but are appreciated for their availability and for coming from an EU Agency rather than purely for the presented expertise. ENISA's low visibility and perceived limited technical expertise were named as the reasons for this.

There is little evidence to suggest that ENISA is being considered as a reference point by its various stakeholders and is recognised for its expertise across the EU. In the interviews only a few stakeholders said that they would consider ENISA to be a centre of expertise. However, Member States and representatives from the EU institutions mostly saw ENISA as a valuable partner at EU level supporting coordination and capacity building. They did not consider ENISA as a source of expert knowledge. Among private sector stakeholders, ENISA has limited visibility and has not become known as a reference point for advice or assistance, as shown by the evaluations of ENISA's activities in 2014 and 2015, as well as confirmed by the interviews.

Moreover, among the respondents to the open public consultation, the regularity of interaction with ENISA and use of the Agency's products and services varies between the stakeholders. While 51% (33 out of 65) interacted with ENISA's products and services a few or only two times per year, 46% of respondents (30) interacted with ENISA on a weekly or a monthly basis. A

comparison across the three groups of respondents shows that national authorities interact with ENISA or use its products and services more regularly than respondents from the group of private enterprises and business associations or other respondents (see Figure 16). Among national authority respondents, 47% interact on a weekly basis, while the largest proportion (50%) of private enterprise and business association respondents do so a few times per year and 35 % of other respondents interact one to two times per year.

Figure 13: Frequency of interact with ENISA or usage ENISA's products and services, (n=65)
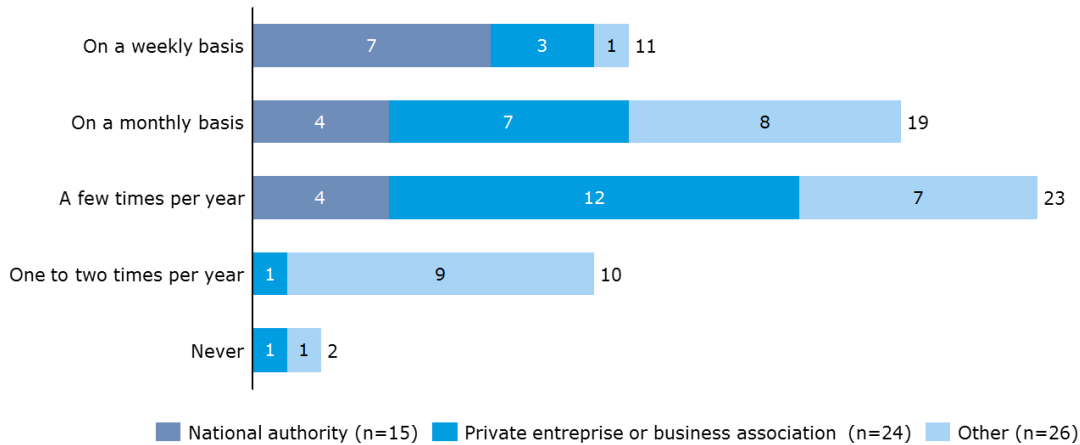
Source: Open public consultation

From a list of eight of ENISA's products and services, the most frequently mentioned as having been used by respondents to the open public consultation in the period 2013-2016 were ENISA's "Guidelines & recommendations, including on standards" (90% or 56 respondents) and the "Reports (e.g. NIS Threat Landscape) & Research Publications" (86% or 53 respondents). This reflects some interest by the stakeholders in the publications of ENISA. Responses were very similar across the three respondent groups: national authorities, private enterprises and business associations and other. Products and services less frequently mentioned as being used were "Article 14 requests" (which are only available to Member States and the EU institutions), "training material or toolkit" (in particular rarely indicated by private enterprises or business associations as being used) and "training or workshop opportunities" were least indicated as being used by 'other' respondents.

The most frequently given reasons for using ENISA's products were "The products and services are provided by an EU-level body" (83% or 52 respondents), "The products and services are free of charge" (67% or 42 respondents) and "The products and services can be trusted" (63% or 40 respondents). Respondents were asked to select out of a list of eight options. This suggests that the expertise presented in ENISA's publications and services is recognised, but is a secondary consideration relative to their availability and the trustworthiness which seem to stem from the fact that it is an EU level body.

Figure 14: Reason for using ENISA's products/services, (n=63), multiple choice question
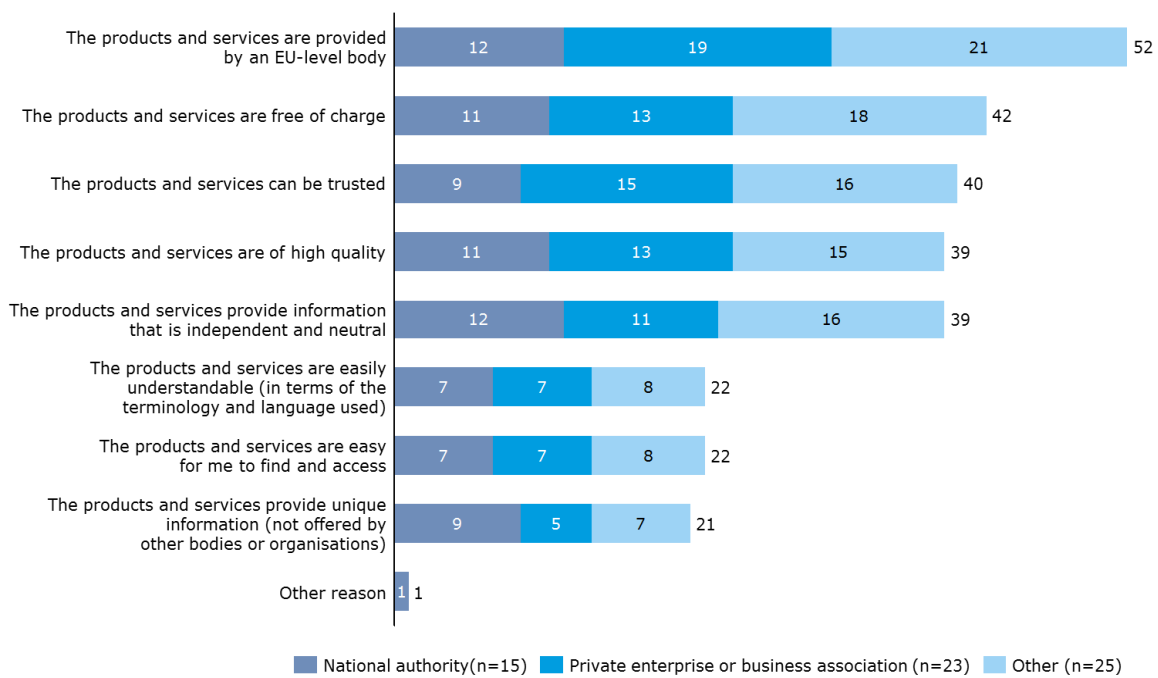
Source: Open public consultation

Little visibility and lack of expertise impede ENISA becoming a centre of expertise and a reference point for stakeholders. Most importantly, compared to other EU agencies, ENISA has little visibility and most stakeholders doubted that ENISA had been able to develop its own brand as compared to Frontex or Europol (EC3). Without being sufficiently known across the EU, it will not be possible for ENISA to be considered as a central source of guidance, advice and assistance. The 2015 evaluation of ENISA's activities found that the Agency could improve its effectiveness by ensuring better dissemination of events and publications in order to reach a larger audience and increase its visibility. Interviewees also criticised the Agency for its limited expertise, in particular in the technical fields. The findings also show that ENISA struggles to hire experts which can be explained by a combination of factors: there are general difficulties across the public sector to compete with the private cybersecurity sector when trying to hire experts; ENISA's human resource policies over the period 2013-2016 did not function well (see section 3.2.2.8.) and, for some experts, Greece as a location seems to be less attractive, e.g. in terms of spouses being able to find work (see section 3.2.2.10).

3.2.2.5   Effectiveness at setting its work priorities

EQ6: How effectively has the Agency managed to set its work priorities?
ENISA sets its annual work programme one year ahead – the work priorities are determined by the Management Board with input from ENISA's management and to a limited extent the PSG. As a result, the work priorities primarily reflect the interests and needs of Member States (as ENISA's main clients) over those of other stakeholders, e.g. industry, the Commission and the EU more widely. Due to divergences in priorities at national level, the work programme often reflects what is least controversial to Member States and risks representing the lowest common denominator.

Changes in the work programmes from one year to the next, linked to ENISA's broad mandate, mean that there is a lack of continuity in many of ENISA's activities from one year to the next, namely due to the annual (rather than multi-annual) nature of its programming.

ENISA's work priorities primarily reflect the interests of Member States and not necessarily the needs of all relevant stakeholders; they are set by the Management Board in an annual work programme with input from ENISA. ENISA's work is based on annual planning. The work programmes are set up in consultation with the Management Board which is primarily made up of Member States, but also representatives of the Commission and observers; Member States provide comments on the programme that is initially set out in draft form by ENISA. PSG members have a lesser say than in the past – their views are expressed through the ad hoc group of certain Member State representatives and PSG members.[41] The work programme's structure underwent changes in 2015 – in 2013 and 2014 the work was divided across three work streams that changed on an annual basis with given activities being planned within these, while from 2015 onwards strategic objectives were set out that remain the same year-on-year. Additionally, Horizontal Operational Activities are conducted. KIIs are set by the Management Board for the work plan activities - they are followed up on through the annual activity reports. The process was judged by a few interviewees as being long, tedious, time consuming and burdensome, occupying much of ENISA managements' time when it is being set.

When commenting on the effectiveness of the process, ENISA staff and users and advisors, as well as some PSG members pointed to the fact that Member States were key in determining ENISA's work priorities, sometimes at the expense of the needs and interests of other stakeholders, e.g. industry, the Commission and the EU more broadly. Moreover, it was felt that due to competing interests among larger, more experienced Member States and smaller, less resource-rich Member States, ENISA's work programme risked representing the lowest common denominator and being diluted. Standardisation and certification were referred to as two areas where Member States had their own national plans and resist ENISA getting involved. Some areas that ENISA should be focussing on more as priority areas than is currently the case, according to industry stakeholders in particular, included the Internet of Things, the move to big data and machine intelligence, certification, becoming more active in the educational field, e.g. by supporting the creation of Massive Open Online Courses (MOOC) in the field of cybersecurity.

It was suggested that more room could be integrated into ENISA's work programme to allow for it to respond to the ad hoc needs of the Commission and to unforeseeable events/needs. A few interviewees from ENISA staff and ENISA's users and advisors suggested that ENISA itself could be given the possibility to determine part of the work programme.

ENISA's work programme covers a wide range of activities and sectors, and there is a lack of continuity in many of its activities from one year to the next. The Cyber Europe Exercises and the threat landscape were cited as the two main activities that are repeated regularly; others change on an annual basis, leading to a lack of continuity and the inability for ENISA staff to develop in-depth expertise in given areas. This is also a reflection of the annual (rather than multi-annual) nature of the way ENISA sets its work priorities. The 2015 evaluation supported these findings with the broad mandate of the Agency and the variety of tasks it seeks to fulfil being perceived by stakeholders as a limiting factor to its effectiveness. In the open public consultation, stakeholders suggested that ENISA should keep a clearer focus on priorities and avoid taking on additional tasks that represent a burden for the staff members.

3.2.2.6   Tackling upcoming, unplanned issues

EQ7: How effectively does the Agency tackle important upcoming, unplanned issues derived from the demands of its constituencies and/or EU policy priorities?

---

[41] The PSG representatives are not formal members of the Management Board and primarily have an advisory role vis-à-vis the Executive Director.

ENISA is able to respond to upcoming, unplanned issues based on stakeholder demands or EU policy priorities through Article 14 requests and amendments to its work programme. These options are considered to be effective, though there is room for more flexibility in order to further consider the needs of stakeholders other than Member States, in particular those of the CERT/CSIRT community, and resource constraints mean it has to prioritise.

Article 14 of ENISA's Regulation allows it to respond to the upcoming needs of its key stakeholders to a degree Based on Article 14, the European Parliament, the Council, the European Commission and a competent body appointed by a Member State can submit a request for advice or assistance falling within the Agency's objectives and tasks. These requests have to be addressed to the Executive Director who then informs the Management Board and the Executive Board to take a decision whether the requested advice or assistance can be provided. Requests can be within the scope of what ENISA already does (e.g. the provision of a specific training course) or cover new areas as long as they are within the remit of the Agency's mandate. The stakeholders concerned expressed satisfaction with the provision. However, ENISA staff and management noted that it was not possible to respond to all requests within the limits of the Agency's budget and human resources. Therefore, requests had to be carefully considered and some requests were not responded to.

Between 2013 and 2016, ENISA responded to a total of 63 requests submitted under Article 14. Over the years 2014 and 2015, requests were received from 17 different Member States, the Commission, the Council of the European Union, the European External Action Service, CEPOL and a third country. Member States' requests primarily concerned training for CERTs/CSIRTs or other public bodies. Requests also concerned the implementation of topical workshops, support with developing a cybersecurity strategy for an entire Member State or on specific topics.[42] Among the respondents to the open public consultation, "Article 14 requests" were one of the services that were less frequently mentioned as being used. Only five out of 15 responding national authorities reported that they had used Article 14 requests over the period 2013-2016. However, the actual number of different Member States having used the services shows that in fact, the requests are used more often. On average, the response to one request costs EUR 15,000. There is however no clear relation between the number of requests responded to per year and the total costs.

Table 15: Overview of Article 14 requests

	2013	2014	2015	2016
Number of new Article 14 requests	13	12	23	15
Total cost of Article 14 requests	€ 200,000	€ 317,637	€ 210,957	€ 229,107

The presented data shows that Article 14 requests are employed to receive support from ENISA and the Agency is able to use them as a means to respond to needs that were not foreseen at the moment the work programme was set up.

ENISA's work programme and activities can be amended to allow the Agency to react to upcoming, unplanned events. Although adopted well in advance, ENISA's work programmes tend to evolve during their year of implementation. A structured process is in place allowing the Management Board to modify the work programme and reallocate financial and human resources when needed. This flexibility was positively viewed by a variety of stakeholders. However, there is room for more flexibility in order to further consider the needs of stakeholders other than Member States. The fact that the work programme needs to be drafted one year in advance, and does not allow for greater flexibility to respond to ad hoc requests, was perceived by a number of

---

[42] ENISA (2016) Activity Report 2015 and ENISA (2015): Activity Report 2014.

interviewees as a limiting factor to the Agency's effectiveness and ability to respond in such a fast paced area as NIS with changing political priorities at EU level. A few survey respondents pointed to this rigidity in their comments on ENISA's organisational set-up, stating that it blocked resources and did not allow the Agency to contribute to emerging issues. It was suggested that part of ENISA's budget should be set aside to allow it to respond to emerging challenges.

However, additional activities (which fall outside the work programme) undertaken by ENISA's staff reflect its ability to tackle unplanned issues. This includes the preparation of Info Notes or ENISA internally deciding to produce papers in response to policy discussions as part of its role as an advisor to the EU institutions. As these activities are not foreseen in the Agency's work programmes, they rely on the motivation of ENISA's staff to take on additional tasks.

Moreover, among the respondents to the open public consultation, 87% (54 respondents) agreed that ENISA's products and services over 2013-2016 had to a large or to some extent responded to the emerging needs of the cybersecurity community in a timely manner. As Figure 15 below shows, this was a consistent assessment across all respondent categories.

Figure 15: Extent to which ENISA's products/services over 2013-2016 responded to emerging needs of the cyber-security community in a timely manner, (n=62)
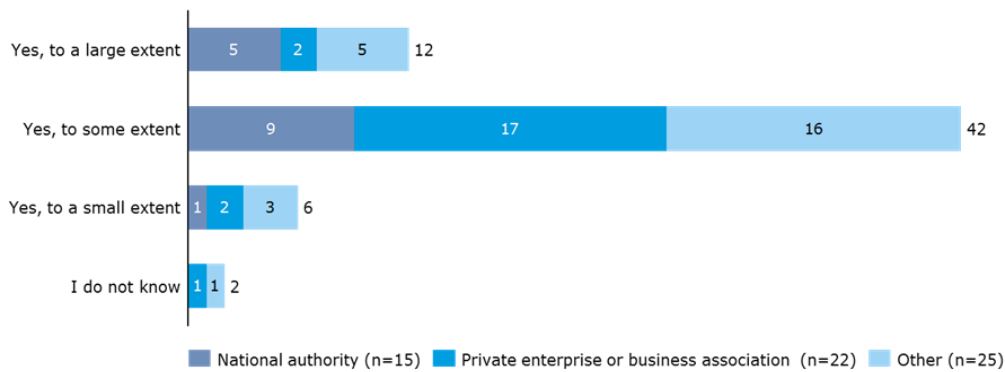
Source: Open public consultation

Limitations in ENISA's flexibility to respond to unforeseen issues stem from the Agency's limited resources. With generally scarce resources, ENISA's management needs to carefully consider whether and to what extent Article 14 requests can be covered. According to interviewees, this can lead to situations where there is competition between the completion of the work programme as agreed with the Member States and any ad hoc request submitted by an EU institution. In fact, the CERT/CSIRT community expressed little satisfaction with ENISA's ability to react to unplanned issues. Interviewees from the Member States and EU institutions and bodies suggested that they would seek support within their own community in case of unplanned, short-term requests rather than address these to ENISA. Due to its limited resources, it was judged that the Agency would respond to ad hoc requests with significant delay or not at all. In particular, in the context of ENISA's new responsibilities under the NIS Directive, an important amount of the Agency's budget will be fixed and cannot be moved to respond to unplanned issues.

3.2.2.7   Quality level of tasks over time

EQ8: Does the Agency consistently perform the same tasks with the same quality level over time?
Overall, the tasks performed by ENISA meet minimum quality expectations, though mixed feedback was provided on the quality and utility of its reports. Moreover, the evaluation identified a varying degree of utility of the Agency's outputs depending on the needs of the different stakeholder groups.

ENISA's performance generally meets quality standards but does not seem to exceed these. Interviewed stakeholders provided mixed feedback on the quality level of the Agency's work, notably of its reports. A number of interviewees – across all stakeholder groups - suggested that the degree of usefulness and quality of ENISA's reports/publications varied and that they did not necessarily "bring a unique selling point". While a few Member State interviewees considered the reports which summarise information from several Member States and provide an independent EU perspective to be very useful, others suggested that the utility varied depending on what was available at national level. Among the open public consultation respondents, 62% (39 out of 63) indicated that they used ENISA's products and services because they were of high quality. Among national authorities, 73% (11 out of 15) indicated to use products and services due to their high quality. This was not among the most selected reasons by respondents, but national authorities in particular selected this response. It was suggested by one interviewee that to improve the quality of reports, ENISA could draw more on the expertise of national cybersecurity experts from national authorities, academics and the private sector to assist them in developing reports/publications in-house through a peer review process; such a practice would allow it to draw on a wider net of expertise to produce more tailored outputs. Another interviewee suggested that there could be a more structured approach to the selection of expert contributors to publications, thereby ensuring that this is a more European undertaking representing the cybersecurity point of view of Europe. Respondents to the open public consultation also suggested that ENISA could increase the quality of publications by covering less topics but more in-depth. In general, stakeholders showed to be very understanding when it came to smaller issues such as difficulties at the start of a cyber exercise.

As can be seen in Figure 16 below, the quality control mechanisms in place were seen by 76% of respondents to the survey of ENISA's staff and direct stakeholders (65 out of 86) as ensuring a high and consistent quality in ENISA's work and publications "to some" or "to a high extent". They were seen as doing so only "to a limited extent" or "not at all" by 9% of respondents (8 out of 86). ENISA staff were slightly more critical than the average in considering the quality control mechanisms as only ensuring such quality "to a limited extent" or "not at all" (14%).

Figure 16: Extent of agreement or disagreement with the following statement on quality control mechanisms
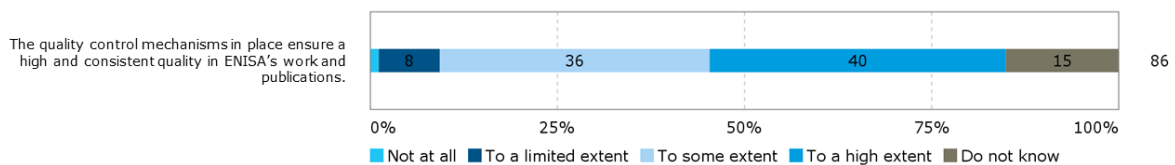
Source: Survey of ENISA staff and direct stakeholders

Seven survey respondents provided additional comments, all of them referring to low or non-existent quality control mechanisms.

3.2.2.8   ENISA's effectiveness considering its governance structure, organisational structure and HR policies

> **EQ11: How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to effectiveness in the work of the agency?**
>
> **ENISA's governance structure,** with a Management Board, an Executive Board and the PSG, is conducive to the effectiveness of its work, though there is room to increase its representativeness and effectiveness by, for example, giving the PSG a more formal role, delegating power within the Management Board to smaller groups, allowing the Executive Board to take on a more pro-active role, and formalising the role of the NLO network.

Its **internal organisational structure** contributes to the effectiveness of its work through its management practices, small size which leads to a lack of complexity, separation along thematic lines and relatively flat structure. That being said, reorganisations, while necessary to ensure renewal, risk posing a limit to its effectiveness when too frequent; here a balance is necessary.

The **human resource (HR) policies and practices** of ENISA are a key limiter to effectiveness in that ENISA had weak HR policies and practices in place over the 2013-2016 period, with a formal HR department only being set up in late 2016. ENISA also suffers from difficulty recruiting and retaining staff due to both internal (i.e. slow recruitment procedures in a fast-paced, competitive environment; a lack of career progression prospects) and external factors (i.e. constraining staff management rules (e.g. number of contract agents (CAs) versus temporary agents (TAs)); an expertise shortfall in the sector; a lack of competitive salaries in an area that is dominated by demand from the private sector).

ENISA's governance structure is conducive to the effectiveness of its work. The current governance structure, with a Management Board, an Executive Board and the PSG Group (see section 1.2.2 for a description of the governance structure), was seen as conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives) by the large majority of ENISA's direct stakeholders (85% or 75 out of 88 survey respondents) (see Figure 17 below). The interviews with staff and direct stakeholders supported this finding, suggesting that the structure "worked well", "was reasonable", "was adequate", and represented well the views of different stakeholders.

Figure 17: Extent of agreement or disagreement with the following statement: To what extent do you agree/disagree with the following statement: The current governance structure, with a Management Board, an Executive Board and the PSG is conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives)?
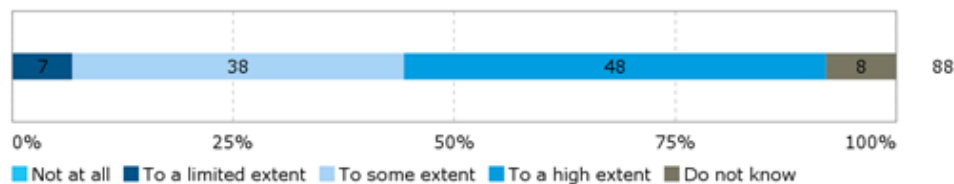
Source: Survey of ENISA staff and direct stakeholders

Key areas for improvement referred to by interviewed stakeholders concerned increasing the representativeness/effectiveness of the governance structure by:
- **Giving the PSG a more formal role**: While it was acknowledged that Member States were ENISA's main client and it therefore made sense for them to be the key players in the governance structure, it was also stated that "as [ENISA is] an internal market agency, the role of Member States versus the rest [e.g. industry] could be slightly more balanced". To ensure this balance, a few interviewees from ENISA staff and among the direct stakeholders suggested giving the PSG (industry) a more formal role and having it feed more into the Management Board's plenary meetings[43].
- **Delegating power within the Management Board to smaller groups**: The Management Board functions in a traditional manner, giving one place and one vote per Member State in plenary meetings. There are different levels of engagement and agendas among the Member States, and ENISA could consider doing like in other agencies and create sub-sets of the

---

[43] Until 2013 (i.e. ENISA's mandate revision) there were three Management Board members representing consumers, industry and academia - they had no voting rights but had a voice; this was no longer the case at the time of writing. Through a non-formal approach, there is an attempt for three rapporteurs from the PSG to attend the Management Board meetings to have a voice. The PSG has an advisory role relative to the Executive Board and the Management Board listened to/exchanged views with them through an ad hoc group of Member States and PSG representatives.

Management Board to discuss given topics according to needs and the level of interest before discussing it in plenary form to make the process more streamlined and effective. This has been done with the Executive Board to a certain extent, but it can only prepare advice and assist the Management Board so it is confined to administrative, not policy matters.

- **Providing a more pro-active role to the <u>Executive Board</u>**: The addition of an Executive Board was seen as a positive development, though one interviewee suggested that the structure could be streamlined so that the Executive Board could react to a certain need when it arose and be used in more areas to ensure further flexibility.
- **Formalising the role of the <u>NLO network</u>**: The <u>NLO network</u> was also viewed as a positive element of the governance structure, but it was felt that its role needed to be more formalised[44]. The findings of the 2015 evaluation point to the fact that different NLOs view their role differently and are more or less active at, e.g. disseminating ENISA's publications to national stakeholders.

ENISA's internal organisational structure was overall perceived as contributing to the effectiveness of its work, though frequent reorganisations limited its effectiveness. A high proportion of respondents to the survey (80% - 70 out of 88) saw ENISA's organisational solutions and procedures as adequate to some or to a high extent (see Figure 18 below). However, ENISA staff (including management) was more critical of the organisational solutions and procedures relative to the direct stakeholders - a quarter (25%) considered them to be only adequate to a limited extent or not adequate at all. Frequent internal reorganisations, limited professional development opportunities and an unclear evidence base being used for decisions related to the allocation of work to given individuals were cited as some of the problems faced.

Figure 18: Extent of agreement or disagreement with statement regarding ENISA's organisational solutions and procedures
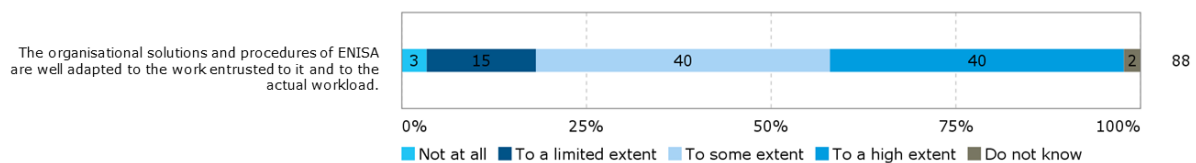
Source: Survey of ENISA staff and direct stakeholders

The interviews with staff and Executive and Management Board members supported these findings with the internal organisational structure being qualified as "adequate for a small organisation", "rather flat and with an open atmosphere", "not very hierarchical", "not too complex because of the small size of the teams", "the separation along thematic lines working well", and the ability to avoid overlap by working together. Should the Agency grow in size, it was suggested that a further clustering of the operational department may be necessary along the lines of national agencies like ANSSI, the German Federal Office for Information Security (BSI) etc. Moreover, reference was made to organisational reorganisations leading to a lack of continuity in activities and dissatisfaction among staff. However, views were also expressed as to the necessity of reorganisation for renewal, e.g. the end 2016 reorganisation involved bringing in a "stakeholder relations" aspect to ENISA's architecture to support less technical aspect to their work/communications.

Moreover, a majority of survey respondents (73% or 64 out of 88 respondents) saw ENISA's management practices as conducive to creating an effective organisation (i.e. in terms of meeting its objectives) to some or to a high extent. Management Board members were generally more positive than the other stakeholders, with 63% indicating that ENISA's management practices are conducive to creating an effective organisation "to a high extent". Some concerns were expressed by respondents who rated these practices more negatively, citing unjustified decisions, the

---

[44] The NLO network is not defined in the ENISA Regulation.

expression of personal agendas and ENISA staff not being allowed to express themselves fully and freely as reasons for this assessment.

Figure 19: Extent of agreement or disagreement with the following statement: ENISA's management practices are conducive to creating an effective organisation (i.e. in terms of meeting its objectives)?
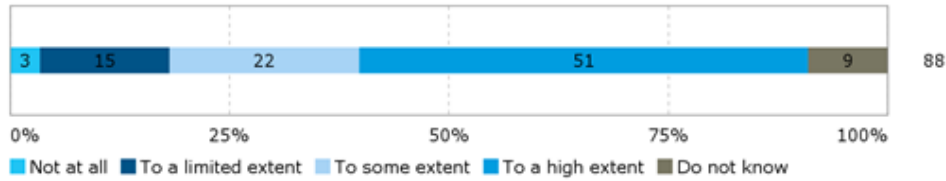
Source: Survey of ENISA staff and direct stakeholders

ENISA had limited formal HR policies and practices over the 2013-2016 period. While the recruitment and training procedures were seen as appropriate to some or to a high extent by 52% of respondents to the survey to ENISA staff and direct stakeholders (46 out of 88), they were seen by 33% of respondents (29 out of 88) as not being appropriate or only being appropriate to a limited extent for ENISA's workload (see Figure 20 below). ENISA staff (including management) were more critical than the direct stakeholders vis-à-vis the recruitment and training procedures, with more than half of them (52%) regarding them as only adequate to a limited extent or not at all. Problems linked to the recruitment process were mentioned by 13 respondents. They criticized the process for being too slow and therefore not being adapted to the cybersecurity domain. It was stated that technical experts were being sought out heavily in this area and could not wait so long for a positive answer or a confirmation from ENISA. The lack of training that the staff experienced over the past five years due to the Agency not having an HR office was the second most mentioned issue, with 12 respondents providing comments on this topic. In the field of cybersecurity, which evolves fast, a lack of training was perceived as very detrimental as it did not allow ENISA staff to stay up to date with the most recent developments. In contrast to these findings, the 2013 and 2014 annual reports state that the Agency complies with the three assessment criteria for the internal control system, where the first criteria is "staff that have the requisite knowledge and skills".[45]

Figure 20: Extent of agreement or disagreement with statement regarding ENISA's recruitment and training procedures
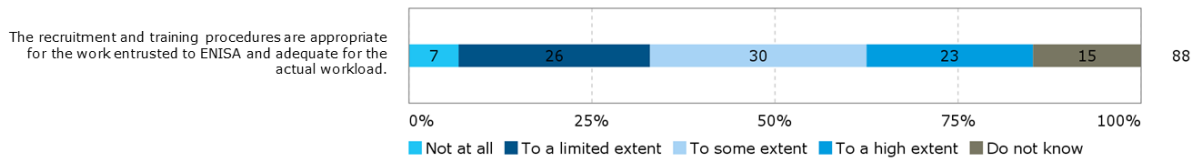
Source: Survey of ENISA staff and direct stakeholders

The interviews with ENISA staff and management revealed that ENISA has weak HR policies and practices in place, with a formal HR department only being set up in late 2016. The appointment of a formal HR manager was very positively viewed and hopes were expressed by many interviewees that HR practices and processes would be prioritised further in the future.

ENISA has difficulty recruiting and retaining staff. The recruitment issues that ENISA faces are more significant than in most of the other EU agencies and bodies that ENISA was compared to as part of the benchmarking exercise. The data presented below, which compares the share of unfilled staff posts of 2014 and 2015 across a selection of EU agencies and bodies, points to the fact that ENISA has been unable to fill the same number of posts over the two year period and is the agency with the second highest number of unfilled positions.

---

[45] Annual activity report 2013, p.40; Annual activity report 2014, p.59

Figure 21 : Comparison of share of unfilled staff posts for a selection of EU agencies, 2014 and 2015
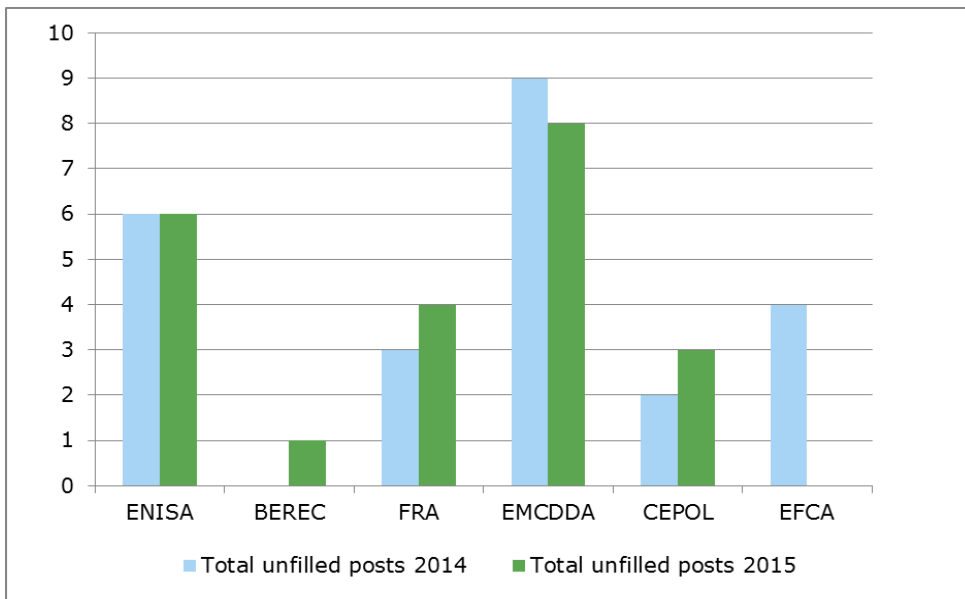
Source: Source of data: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III Bodies set up by the EU and having legal personality and Public-Private Partnership.

The same development is also visible in Figure 22. ENISA's share of filled staff positions has gradually decreased in comparison to FRA and EMCDDA who were able to maintain a fairly consistent percentage of filled positions across 2014-2016.

Figure 22: **Compared share of staff positions filled on an annual basis for ENISA, FRA, and EMCDDA, 2014-2016**
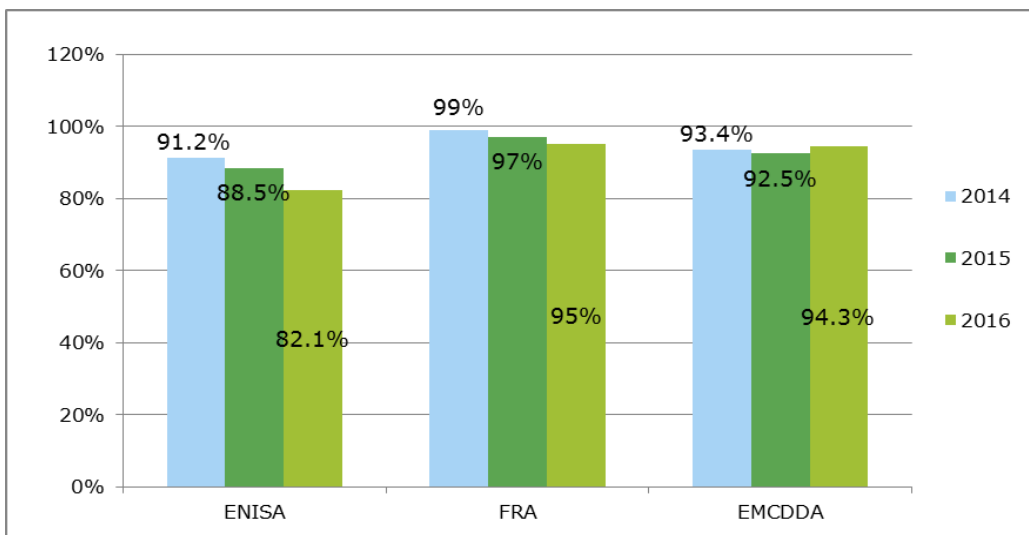
Source: Data gathered through secondary sources and received by ENISA, FRA and EMCDDA.

A number of factors have been identified that lead to ENISA's issues in recruitment and retaining staff. The interviews with ENISA staff and management pointed to the fact that ENISA has difficulty recruiting and retaining staff due to a number of factors including:

- constraining staff management rules (e.g. number of CAs versus TAs);
- an expertise shortfall in the sector;
- a lack of competitive salaries and attractive contract conditions in an area that is dominated by demand from the private sector;
- slow recruitment procedures in a fast-paced, competitive environment;

- a lack of career progression prospects due to the size of the Agency and limited turnover at the Head of Unit level;
- perceived barriers to integration for experts from outside Greece, including difficulties for spouses to find work (due to the language barrier, the economic crisis), and insufficient schooling options

It was further mentioned that in other public sector organisations a more flexible structure has been created to keep people (e.g. legislation has been introduced to pay people more in a number of Member States, being more adaptable in the work arrangements offered like teleworking, offering a train package, or packages for the children of staff), but doing this within the confines of the EU institutions and legislation proves a challenge. This was also confirmed by ENISA's annual activity reports, where the main reasons for difficulties in recruiting and retention are attributed to the types of post that are being offered (CA posts), the low coefficient factor which applies to salaries of ENISA employees in Greece (AAR:2015:50), and the absence of international schooling for the children of Agency staff (AAR:2014: 31, AAR:2015:50).[46] The survey also supported this finding when respondents were asked about the size of the Agency, which was the element of ENISA's organisational setup that was judged the most strongly by survey respondents (Figure 23 below).

Figure 23: To what extent do you agree/disagree with the statements below regarding ENISA?
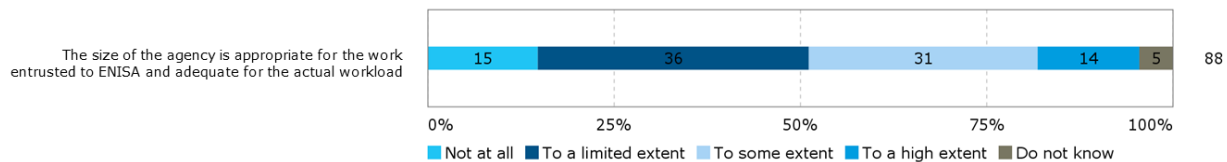
Source: Survey of ENISA staff and direct stakeholders

ENISA staff (including management) was much more pessimistic about the size of the Agency being adequate than other respondent types, with 61% of them regarding it as adequate only to a limited extent or not at all. A large number of those respondents (35) that were more negative in their assessment referred to the need to have more staff (this was mentioned by a variety of respondent types, including six Management and Executive Board members, 21 ENISA staff members, two NLOs and five PSG members). They called for the need for "more operational experts" and expressed their concern related to hiring being frozen. They explained in detail the difficulties faced in recruiting staff willing to work in Greece and the negative impact on hiring of the lack of facilities for international families in Heraklion and Athens.

The table below presents an overview of ENISA's staff composition. A significant increase can be noted between 2014 and 2015 in the number of CA.

Table 16: Staff by category end of year

Staff category	2011	2012	2013	2014	2015
Administrators	26	27	27	34	32
Assistants	15	15	16	14	16
Contract agents	13	12	13	15	24
Seconded national experts	4	4	3	5	3
Total	58	58	59	68	75

---

[46] These issues are not raised in the 2013 annual activity report, except for a reference to a shortage of staff in connection with the Internal Control Coordinator role. Furthermore, this report states that "adequate measures" are in place to ensure business continuity, also in relation to staff (sick-leave, holidays, etc.) (AAR:2013:38).

A comparison with other EU agencies and bodies also shows the increasing reliance within ENISA on CAs and a low number of seconded national experts (SNEs). As presented in Figure 24, ENISA has the highest share of CAs among the agencies and bodies considered as part of the benchmarking exercise conducted for this study. In addition, ENISA employs comparably few SNEs. In interviews, a need was expressed to ensure better exchange between ENISA and the Member States. An increase in the number of SNEs up to the level of other agencies could be a response to this request.

Figure 24: Average distribution over staff categories, 2014-2016
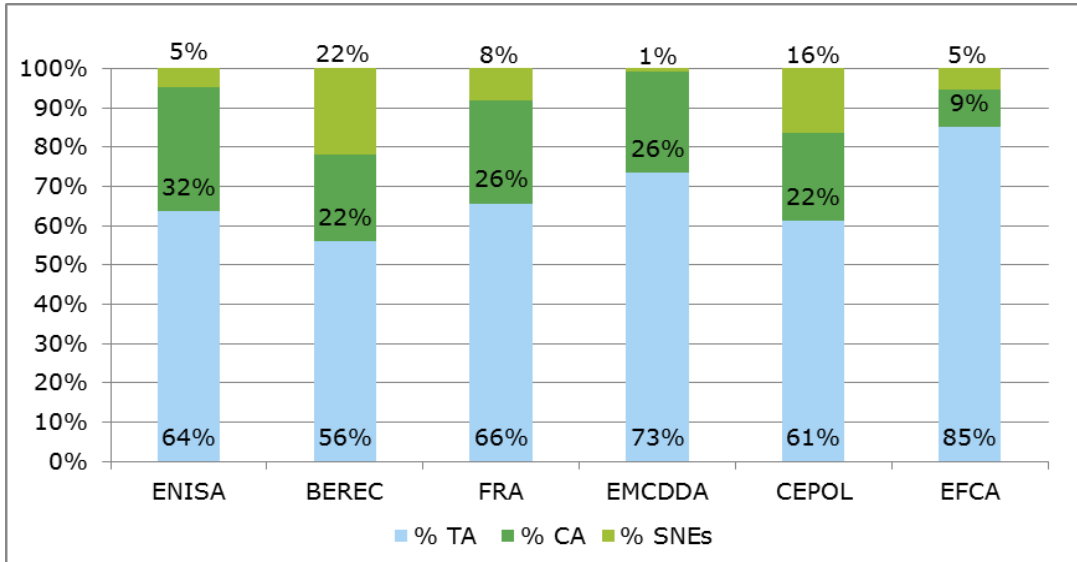
Source: presentation by Ramboll, data from European Commission: Draft General Budget of the European Union for the financial year 2017 - Working Document Part III

Over the period 2014-2016, ENISA had the highest percentage increase of CAs compared to the other agencies, reflecting the efforts to reduce staff expenditure. The share increased by 120% for ENISA. As presented in Figure 25 below, BEREC and the EFCA went through a very similar development between 2014 and 2016 in which some of the SNE positions were replaced with CAs.

Figure 25: Percentage change in budget allocations for different staff categories, 2014-2016
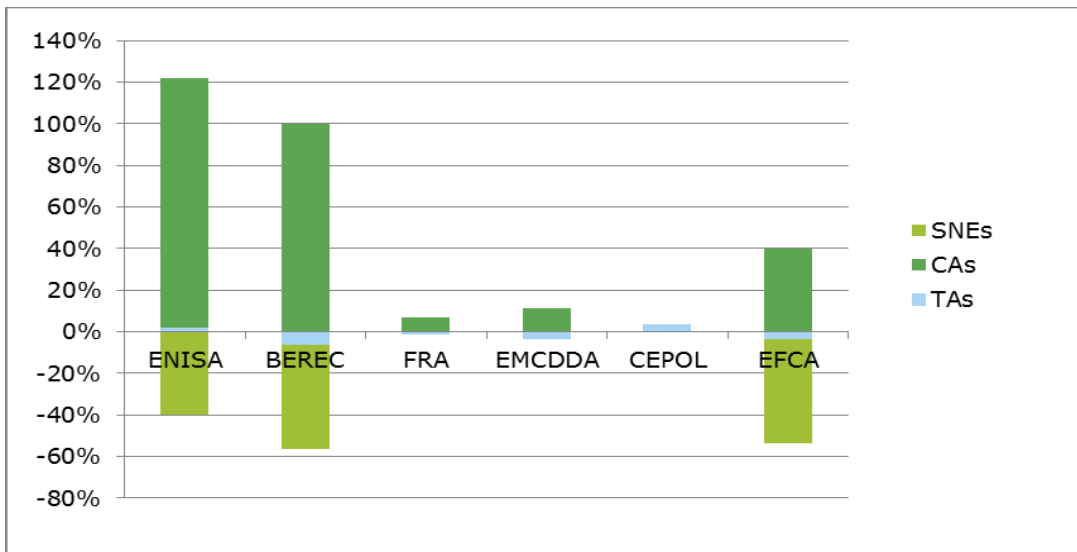
Source: presentation by Ramboll, data from European Commission: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III

Nevertheless, 65% of respondents to the survey to ENISA staff and direct stakeholders (57 out of 88) saw staff composition as adequate for ENISA's work to some or to a high extent and 30% of respondents (26 out of 88) saw it as only adequate to some extent or not at all (see Figure 26 below). ENISA staff (including management) were more likely to express a more negative view than the direct stakeholders. A number of respondents felt that there was a need to develop internal expertise through the hiring of more senior staff. The balance between administrative staff and operational staff was also seen as an issue by seven respondents, who said that there was a clear need for more technical staff hires. Finally, one respondent expressed the importance for ENISA staff being more geographically representative of the EU; this view was also supported in the interviews.

Figure 26: Extent of agreement or disagreement with statement regarding ENISA's staff composition
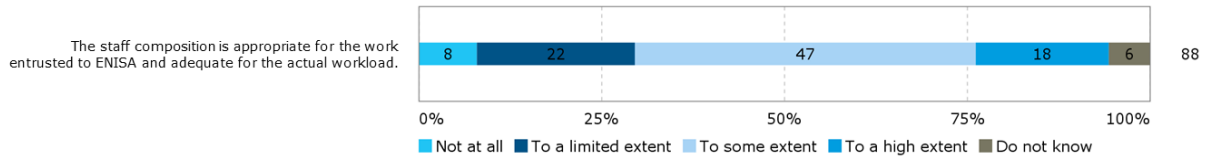
Source: Survey of ENISA staff and direct stakeholders

Vacancies are difficult to fill with the current salary level (basic level for the functional area concerned is 2,476.74 EUR according to vacancy announcements) and limited benefits or allowances. As a consequence, most applicants are either Greek nationals and/or from other parts of Southern Europe, with very few applicants from northern Europe. This is reflected in the staff composition of the Agency (presented in Figure 27 below), with approximately 32% of staff being Greek nationals in 2015.

Figure 27: Nationality of staff members (2013-2015)
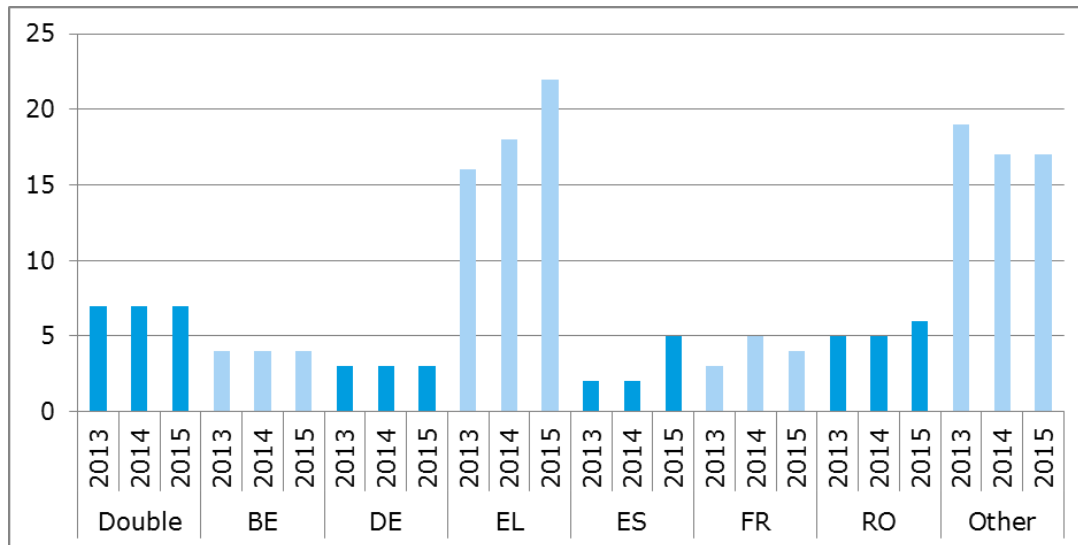
Source: Ramboll Management Consulting based on data from ENISA annual reports

As one interviewee put it: "To compete better, we need to put the HR department at a higher level; vacancy notices should be quicker; we could provide better topics (could be more interesting in our job offers); and in general we should provide a more competitive package in terms of medical scheme and other various things". Another suggested that staff rotations between the EU agencies and with the Commission to make the work more attractive and to bring in new people qualified to work at a higher career level would be a plus.

The findings of the evaluations of ENISA's 2014 and 2015 core operational activities supported these findings. While stakeholders assessed that ENISA's organisational set-up,

procedures and processes were conducive to the achievement of its objectives, a number of limiting factors to its effectiveness were identified, including:

- The limited resources that ENISA disposes of (2014 and 2015 evaluation);
- The broad mandate and the variety of tasks it seeks to fulfil;
- Difficulties with recruiting staff/talent with the needed competence, due to the salaries ENISA can offer and its geographical location.

3.2.2.9   Relationship with its stakeholders

EQ12: How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate?
The evidence shows that ENISA has created strong and trustful relationships with some of its stakeholders, most importantly with the Member States and in particular the CERT/CSIRT community. The evidence suggests that ENISA could further improve the exchange of information between CERTs/CSIRTs by providing an oversight of available knowledge and good practices and by enhancing the coordination of CERTs/CSIRTs at the policy level.
The cooperation and coordination with the Commission's DGs and some of the EU Agencies could be improved to reduce risks of overlap and create synergies. ENISA could also improve cooperation with the industry.

ENISA's direct stakeholders and ENISA staff agree that ENISA ensures successful cooperation with its stakeholders. As can be seen in Figure 28, almost all respondents to the survey of ENISA staff and direct stakeholders (93%) thought that ENISA is open to cooperating with a variety of stakeholders to some or to a high extent, across different levels and sectors, to ensure better results. Two respondents from the Management and Executive Boards and one respondent from the PSG thought that the Agency was only open to such cooperation to a limited extent.

Figure 28: Extent of agreement or disagreement with statement regarding ENISA's cooperation with stakeholders
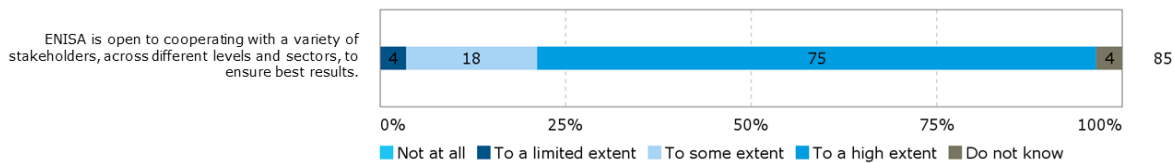
Source: Survey of ENISA staff and direct stakeholders

A majority of respondents to the survey of ENISA staff and direct stakeholders (81%) considered that to some or to a high extent, ENISA has good systems and procedures in place for stakeholder consultation and management, as shown in Figure 29 below. A minority (8%) thought that it only had such good systems in place to a limited extent or not at all. ENISA staff were slightly more critical of these systems than the average, with 12% of them considering that ENISA only had such good systems in place to a limited extent or not at all. The Management and Executive Board members as well as the PSG members were mostly positive (respectively 84% and 92%), saying that ENISA had good systems in place to some or to a high extent or did not know.

Figure 29: Extent of agreement or disagreement with statement regarding ENISA's cooperation with stakeholders
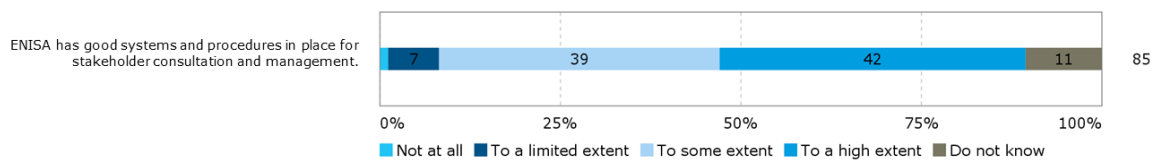
Source: Survey of ENISA staff and direct stakeholders

Almost all respondents (93%) to the survey of ENISA staff and direct stakeholders thought that ENISA had built strong and trustful relationships with its stakeholders when executing its mandate to some or to a high extent (see Figure 30 below). Responses across the different stakeholder groups were very similar.

Figure 30: Extent of agreement or disagreement with statement regarding ENISA's cooperation with stakeholders
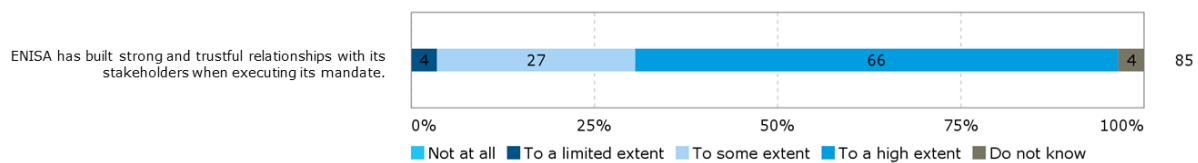
Source: Survey of ENISA staff and direct stakeholders

Open public consultation respondents from national authorities believed that one of the main achievements of ENISA was the support ENISA provided to Member States in particular by fostering cooperation via the share of expertise among Member States. However, it was also suggested that ENISA could do more to share information on which expertise and practices are available in the Member States and can be of benefit to others.

General suggestions were made to improve ENISA's cooperation with its stakeholders. These were found in the surveys, the open public consultation, as well as the interviews and provided by a variety of the different stakeholder groups:

- ENISA should develop more internal expertise to provide better services to its stakeholders. Stakeholders did not refer to specific areas but rather indicated that in general ENISA should have more technical, in-depth expertise, ideally in all the thematic areas covered by the Agency.
- ENISA tends to be very structured in their approach to stakeholders, following the work programme very closely. This limits the possibility for informal interaction or ad hoc cooperation.
- It was recommended that ENISA ensures greater engagement with the PSG and generally ensures a better connection with the industry, for example through public private partnerships.

Cooperation with the EU institutions is in place but there is a lot of room for improvement. In the interviews, stakeholders from the different Commission DGs and other EU institutions explained how they worked together with ENISA and highlighted some positive achievements of this cooperation. Nevertheless, the collected evidence also shows that ENISA's relationships with EU institutions are not sufficiently strong. On the one hand, there is a perception that the Commission DGs do not systematically involve ENISA when they work on matters relating to cybersecurity or data protection. There seems to be some doubt about ENISA's expertise in some areas and a lack of structural cooperation between ENISA and the DGs. On the other hand, ENISA seems to lack resources to take ownership on some of the tasks when sharing responsibilities with the Commission.

The interviews show that ENISA has positive relationships with most of the EU agencies. A topic of raised by many interviewees is the degree of cooperation between ENISA and CERT-EU, which is described in section 3.2.4.1. In general, there is a need for a clearer mandate and delimitation of the role of different EU agencies and bodies active in the area of cybersecurity, including ENISA, CERT-EU, Europol's EC3, but also of the Commission's DG JRC. There seems to be untapped potential for cooperation and exchange of information.

ENISA has developed strong relationships with the Member States. Member States are present in ENISA's Management Board allowing for the involvement in the development of the annual work programmes. ENISA cooperates with the Member States through the NLO network which is intended to serve ENISA as a point of reference into the Member States on specific issues. As shown in the survey results above, the participating members of ENISA's Management Board and the NLOs show a high satisfaction with and trust in the cooperation with ENISA. There are various formats in which ENISA cooperates with the Member States, including exercises, trainings, meetings and the CERT/CSIRT community. A few of the interviewees of ENISA's staff and direct stakeholders considered the complex structures of responsibility for cybersecurity issues in the Member States as a challenge for ENISA, in particular in the context of the upcoming implementation of the NIS Directive, under which ENISA will have to build up relationships with several new groups of authorities in the Member States.

ENISA fosters the cooperation among CERTs/CSIRTs across the EU. ENISA is heavily involved in fostering cooperation between CERTs/CSIRTs, as well as capacity building for CERTs/CSIRTs. In the CERT/CSIRT survey, participants were asked to what extent they thought ENISA proactively supported cooperation among CERTs/CSIRTs during the 2013-2016 period. As can be seen in Figure 31 below, the answers were in large part positive, with 83% of respondents (28 out of 34) thinking it did so to a high or to some extent and 12% (4 out of 34) thinking that it did so to a limited extent or not at all.

Figure 31: Extent to which ENISA proactively supported cooperation among CERTs/CSIRTs during the 2013-2016 period
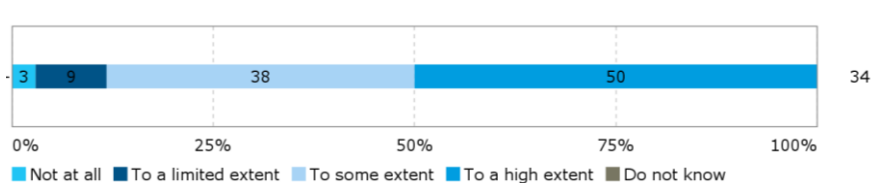
Source: CERT/CSIRT survey

In the survey but also during the interviews, CERTs/CSIRTs provided suggestions how cooperation could be even further improved. It was suggested that ENISA should work on improving how CERTs/CSIRTs exchange information. This could be done by providing an oversight of what expertise and knowledge exist in the CERT/CSIRT community and helping to share good practices and lessons learned from one country to another. Respondents also stressed the importance of "liaising with CERTs/CSIRTs members on the technical level" so as to make ENISA management better equipped to address the needs of the CERT/CSIRT community. At the same time, they suggested that there was a need to reach out to the decision making level of the CERTs/CSIRTs in the Member States and not only focus on the technical level.

ENISA's relationship with further stakeholders, including industry and academia is limited. Among industry and academia stakeholders ENISA is not widely known. Although ENISA publishes reports targeting the industry, for example SMEs, the Agency does not have sufficient outreach to these stakeholders. This was concluded in the evaluations of ENISA's activities in 2014 and 2015 and confirmed during the interviews for the present evaluation. With the PSG there is a formal approach to involving these stakeholders in the planning and decision making processes of the Agency. ENISA's management as well as other stakeholders noted, however, that the role of

the PSG was not sufficiently formalised. Within the Management Board, Member States have the main voice and consequently most of ENISA's activities are targeted towards them (see section 3.2.2.8 for further findings relating to ENISA's governance structure). Respondents from private enterprises and business associations to the open public consultation suggested that ENISA could foster private-public cooperation in the area of cybersecurity.

3.2.2.10 ENISA's effectiveness considering its location

> **EQ13: What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives?**
> ENISA's effectiveness has overall been positively impacted by the move in 2013 of its operations teams to Athens from Heraklion, thereby facilitating access to the Agency from elsewhere and by Agency staff to Brussels. However, its location limits its effectiveness in achieving its policy objectives to a degree as it is more difficult for ENISA's management and staff to organise (ad hoc / informal) exchanges with the EU institutions, thereby affecting the degree of influence it can have on cybersecurity policy at the EU level and its impact in this area. Moreover, the difficulties experienced in recruiting and retaining qualified/expert staff which are partially linked to the Agency's location (see section 3.2.2.8 for further findings relating to ENISA's human resources) limit its ability to recruit and maintain the necessary staff to meet its objective of providing expertise through collating, analysing and making available information and expertise on key NIS issues.

The decision of the seat of EU agencies is a political one, determined by a common agreement between the representatives of the Member States meeting at Head of state or government level or by the Council. An attempt has been made to spread the agencies across all Member States. While in some cases the location decisions taken specify in which city a given agency will be located, in the case of ENISA, only Greece was defined as the location, leaving the decision on the city to the Greek government.[47] ENISA was established in Heraklion. In March 2013, a decision was made to move the operations of the Agency to Athens.

The move of operations to Athens in March 2013 has increased the Agency's effectiveness, though the split between Athens and Heraklion was seen as a limiting factor to its effectiveness. ENISA staff generally saw ENISA's location as less of a hindrance to its effectiveness than other stakeholder types; the move to Athens was overwhelmingly perceived as positive. The main benefit mentioned was that ENISA had become more easily accessible for those visiting the Agency and for staff it had become less time-consuming and expensive to travel across the EU. However, a few ENISA staff (including management) respondents were critical of the fact that the Agency is divided in two (between Heraklion and Athens), which it was perceived hampered internal communication and cohesion.

ENISA's location is limiting its effectiveness in achieving its policy[48] related objectives. ENISA's location was judged by 67% of respondents to the survey of ENISA staff and direct stakeholders (59 out of 88) as enabling ENISA to effectively conduct its work (i.e. in terms of meeting its objectives) to some or to a high extent. It was reviewed as not enabling such effectiveness or only doing so to a limited extent by 28% of respondents (25 out of 88). ENISA's direct stakeholders were more critical than ENISA's staff and management of its location, with the NLOs, the Management and Executive Boards and the PSG members seeing the location as enabling the effectiveness of the Agency to a limited extent or not at all (with 58%, 42% and 39% respectively being of this opinion). By contrast, the large majority of ENISA staff including

---

[47] European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No3 – Agencies' seat and role of the host country. Available at: http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_3_sent_to_ep_cons_2010-12-15_en.pdf

[48] Policy objective: Promote network and information security as an EU policy priority, by assisting the European Union institutions and Member States in developing and implementing EU policies and law related to NIS.

management (84%) assessed the location as conducive to the effectiveness of ENISA's work to some or to a high extent.

Figure 32: Extent of agreement or disagreement with the following statement: ENISA's location enables it to effectively conduct its work (i.e. in term of meetings its objectives)
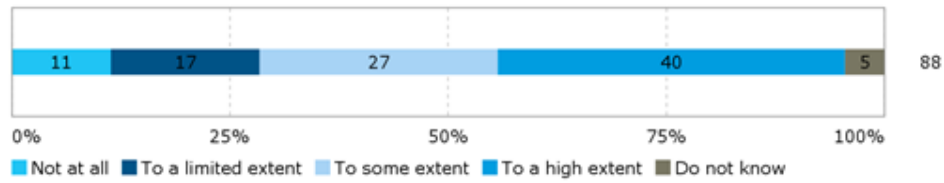
Source: Survey of ENISA staff and direct stakeholders

It was primarily felt by the more critical stakeholders referred to above that ENISA was situated too far from Brussels, making (ad hoc / informal) exchanges between the Agency and the EU institutions more difficult and thereby affecting the degree of influence ENISA can have on cybersecurity policy at the EU level and its impact in this area. The location of ENISA was cited as one source for a lack of coordination with ENISA by several members of the Commission. A number of interviewees across all stakeholder groups were of the opinion that its location limited ENISA's ability to keep its finger on the pulse. It was suggested that the location helped explain why CERT-EU, which is situated in Brussels and can be called upon more easily, is taking on tasks that are could arguably also fall within the mandate of ENISA. Some suggestions for improvement included having a more decentralized office structure though care would need to be taken not to create too much of a fragmented Agency, flexible arrangements with smaller offices where needed, for projects etc., or having a liaison office in Brussels.

In the open public consultation, respondents were asked about the impact of ENISA's split location on the Agency's ability to conduct its work effectively and efficiently. As presented in Figure 33 below, there were very mixed views on this question with 28% (18) judging that the split location affected ENISA's ability to conduct its work effectively and efficiently to some or to a large extent, while 20%(13) felt it did not do so at all. The views were divided among all respondent stakeholder groups.

Figure 33: Extent to which ENISA's split location arrangement affected ENISA's ability to conduct its work effectively and efficiently, (n=65)
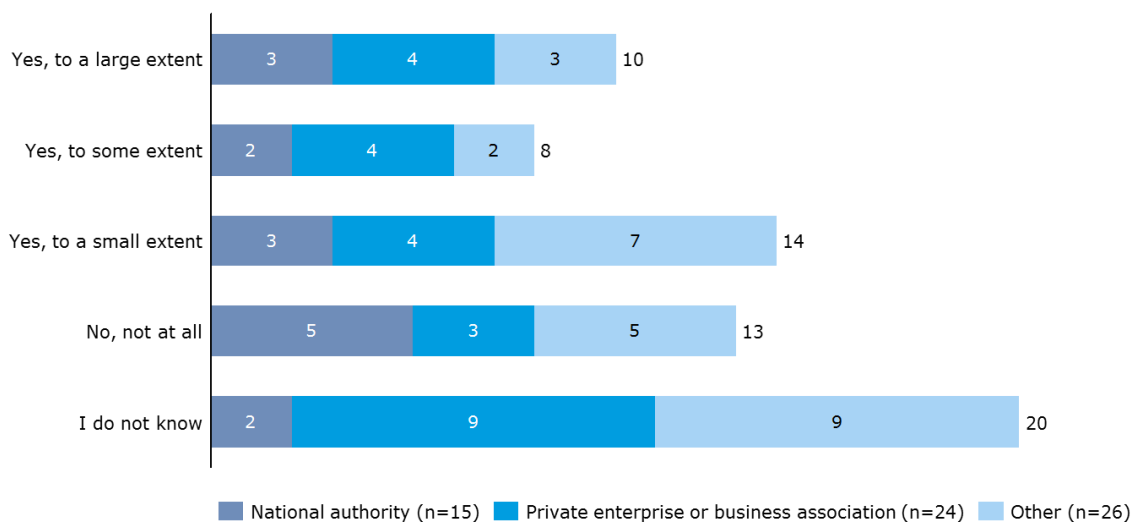
Source: Open public consultation

Respondents were invited to provide a further explanation of their assessment. Respondents who felt more positive about ENISA's current arrangement said that being decentralised from Brussels

provided the Agency an advantage to be perceived as a neutral source of information. Considering that ENISA has still been successful in operating outside its offices and maintained presence and cooperation in relevant events, the location of its offices was not perceived to have affected ENISA's ability to work effectively and efficiently. Respondents who felt less positive about ENISA's current location arrangements said the split location was not optimal for efficiency. Reasons for this included the increase of travel costs as well as costs spent on maintaining both offices. The split location was thought to present a challenge to people management.

ENISA's location limits its effectiveness in terms of its objective to provide expertise[49]. There are several factors influencing ENISA's ability to hire and retain staff but as described in section 3.2.2.8 difficulties for spouses to find work in Greece and the lack of a European school in Athens contribute to the Agency's human resources issues and thus lead to difficulties to provide its stakeholders with the sought after expertise.

3.2.2.11 ENISA's internal mechanisms for programming, monitoring, reporting and evaluating

EQ19: To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc.)?
The programming, monitoring, reporting and evaluating mechanisms implemented by ENISA are adequate to ensure accountability and an appropriate assessment of performance. However, these mechanisms lead to a degree of administrative burden as they are not adapted to the size of the Agency and there is room for improvement in terms of the establishment of a monitoring system that enables the tracking of performance over time against pre-determined KIIs.

ENISA has a series of internal mechanisms for ensuring accountability and the assessment of performance. ENISA's work is based on annual planning and KIIs are set for all activities to evaluate performance. These KIIs are followed up on in ENISA's annual activity reports (section 3.2.2.1 considers ENISA's KIIs to assess effectiveness). The quality assurance of projects is done with a Quality Management System (QMS); the Agency reviewed the QMS in 2015 and 2016. A range of instruments are available to ensure quality such as manuals and guidelines laying down standard operating procedures. Activities follow the Deming Cycle (plan, do, check, act). ENISA has been integrating tools such as electronic signatures, electronic workflows and enterprise resource management. Finally, ENISA has a number of activity-specific tools that it uses to monitor performance, including surveys of participants in the Cyber Europe Exercises and of participants in training sessions. The evaluation of ENISA's 2015 core operational activities (undertaken in the first half of 2016) pointed to some areas for improvement in this regard and assisted ENISA by designing tools for the monitoring of publications via a brief pop up questionnaire, and of the initial and follow-up monitoring of training activities.

ENISA's internal mechanisms for programming, monitoring, reporting and evaluating ensure accountability and an appropriate assessment of the overall performance of the Agency. ENISA carefully follows requirements imposed by the Commission rules and according to reports from the Court of Auditors, the Agency has shown strong compliance and raised no concern with regard to its accountability.[50] ENISA's direct stakeholders, most importantly the Management Board, showed satisfaction with the developed procedures. Also internally (by ENISA

---

[49] Expertise objective: Anticipate and support Europe in facing emerging NIS challenges, by collating, analysing and making available information and expertise on key NIS issues (potentially impacting the EU taking into account the evolutions of the digital environment.)
[50] Court of Auditors (2015): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2014 together with the Agency's reply, and Court of Auditors (2016): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2015 together with the Agency's reply

staff and management), the effectiveness of project planning, project tracking and budget management was considered to be high.

The survey results further confirmed this finding. As can be seen in Figure 34 below, the majority of respondents to the survey of ENISA staff and direct stakeholders (73%) thought that the internal management systems were conducive to effectiveness (i.e. in terms of meeting ENISA's objectives) to some or to a high extent. This effectiveness was viewed as existing only to a limited extent or not at all by 16% of respondents (14 out of 86). Specifically, the members of the Agency's Management and Executive Board were overall satisfied with the effectiveness of these systems, with 84% of them ranking them as leading to effectiveness to some or to a high extent.

Figure 34: Extent of agreement or disagreement with statement regarding ENISA's internal management systems
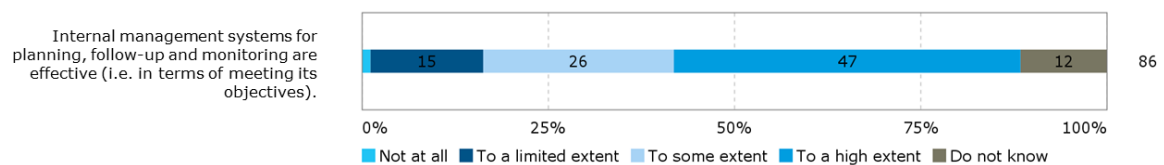
Source: Survey of ENISA staff and direct stakeholders

Requirements to ensure accountability and a review of performance are burdensome for ENISA, in particular considering the small size of the Agency. As an EU Agency, ENISA has to follow the rules and obligations imposed by the Commission. In particular, ENISA's staff and management reported that these requirements represented an important burden as they were not adapted to the small size of the Agency. A quarter of ENSIA staff (25%) indicated in the survey question above that the internal management systems were only to a limited extent or not at all conducive to effectiveness. For example, the Agency works with a high number of rather small projects. Not each of these projects requires the same detailed planning and follow-up as some larger Commission projects would need. Interviewees noted that with limited administrative resources in the Agency it was burdensome to meet all the requirements.

Specific suggestions were made to improve the mechanisms for programming, monitoring, reporting and evaluating:
- Reporting tools should be better integrated with one another and automated to alleviate the burden of administrative tasks. This includes the planning and reporting tools for travel of staff
- The follow up on the use of created reports could be improved. Currently, a focus is set on monitoring the number of downloads of reports. Interviewees suggested that it would be more informative to collect actual feedback from users of reports and to identify how information from reports is being used. Such follow up should take place over several years.
- Members of the Management Board saw artificial constraints created by the requirement to provide an early draft of the work programme by January for the following year. It was reported to be difficult to make specific plans so early in advance and the Work Programme risks to be outdated quickly because the cybersecurity environment is changing rapidly.

The 2015 evaluation also made some conclusions and recommendations in relation to the setting of KIIs which are worthy of note here: **For ENISA, measuring impact is highly challenging and to a large extent dependent on contextual factors, so setting up a monitoring system that works over the long term is essential.** This is true in particular for policy agencies like ENISA, since the impact can only take place in the larger community by stakeholders applying and/or using ENISA's outputs. Moreover, impact can often only really be judged on the longer term through an annual monitoring process. In this respect, ENISA´s annual KIIs are an essential data source when it comes to monitoring the Agency´s impact over time. In comparison to 2014, some of the KIIs for 2015 were more ambitious and provided a better starting point to

measure ENISA´s contribution to reaching the impacts foreseen. However, it should be noted that the actual data needed to measure the KIIs was not available at the time of the evaluation. The reporting on some of the more ambitious KIIs which seek to ascertain "use" is more operational, focussing more on outputs (e.g. the organisation of and number of participants in a workshop) rather than on the actual contribution to an impact (e.g. using ENISA´s recommendations). This is likely to be in part the result of it being too early to judge the true impact of given activities, but also due to a lack of follow-up on a yearly basis in relation to the KIIs set in a given year. On this basis, it was recommended that ENISA set up a monitoring system which seeks to measure performance against pre-defined KIIs set in a given year, allowing for the measurement of impact over a more extended period of time than a year (as is currently the case). Monitoring and reporting in relation to such KIIs would therefore need to be ensured on an annual basis for, e.g. five years. It was further recommended that ENISA ensure that the KIIs capture impact rather than output, and that the collection of data in relation to these is improved.

3.2.2.12 In-house capacity and use of external service providers

EQ20: To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?
The findings are contradictory on whether ENISA has succeeded in building up in-house capacity. Stakeholders strongly differ in their assessment. While the Agency has been able to hire some experts over the last years, ENISA highly depends on external expertise for the implementation of its activities. Decisions to outsource work are made on an individual basis and are only to some extent guided by efficiency criteria.

ENISA strongly relies on external expertise for its activities. From 2014 to 2016, around 80% of the Agency's operational budget was used for procurement of studies. As indicated by ENISA in the benchmarking exercise, in 2016, procurement of study amounted to EUR 1.597.087 of a total operational budget of EUR 2.000.000. Compared to other EU Agencies, ENISA relies a lot more on external expertise. For example, the ratio of operational budget used by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) for procurement of study was reported by the EMCDDA to represent less than 5% in 2013 but has increased to reach slightly over 15% in 2016.[51] Table 17 below provides a detailed overview of ENISA's procurement activities between 2013 and 2016.

Table 17: Overview of ENISA's procurement (operations and non-operations)

	2013	2014	2015	2016
Contracts signed				
Service contracts	18	25	11	12
Specific contracts awarded under re-opening of competition	8	15	20	25
Framework contracts	7	18	19	14
Total number of procurement related contracts	33	58	50	51
Purchase orders				
Issued under a framework contract	78	119	143	127
Not issued under a framework contract	84	115	158	193
Total number of purchase orders	162	234	301	320
Procurement procedures				

---

[51] Information provided by ENISA and EMCDDA for the benchmarking exercise. The agencies were asked to provide the ratio of budget used for procurement of study over the overall operational budget. It has not been possible to verify this information based on other sources.

Open procedures	15	10	9	8
Other procedures	4	20	38	27
Total number of tender procedures	19	30	47	35

Source: Based on Annual Reports, completed and verified by ENISA

From its outset, ENISA is an agency that uses procurement for a lot of its work. With limited human and financial resources, ENISA has to find external capacities to cover the very specific and complex topics of the cybersecurity field as needed by its stakeholders. Often research and data collection is done by external experts, while ENISA staff maintains the responsibility to analyse and report on the collected data. However, some specific tasks are being done internally, such as the cyber exercises, Article 14 requests and the preparation of the implementation of the NIS Directive. A few stakeholders suggested that these tasks would become even more important in the future.

Stakeholders disagree on whether ENISA has successfully built up internal expertise to cover the various tasks assigned to the Agency. While some interviewees (direct stakeholders and representatives from the EU institutions) think that ENISA has managed to hire staff with specific expertise over the past years and see ENISA as being very capable to respond to their needs, other interviewees (of the same group) think that the Agency is significantly hindered to attract the needed expertise as explained in section 3.2.2.8 concerning the effectiveness of ENISA's human resources policies.

The disagreement also concerns the question whether the use of procurement is advisable at all. Some members of ENISA's Management Board said they would like to see ENISA get more work done internally because procurement processes made the Agency slow and dependent on external stakeholders. Others said that ENISA should use its network of experts even more systematically and also involve them in project management roles. This way, staff resources could be freed up for other tasks.

The findings suggest that the "make or buy" choices are made on a case by case basis with no institutionalised consideration of efficiency criteria. According to ENISA staff and management the decision whether an activity is carried out in-house or requires procurement of external services depends on the task and the topic covered. Reasons for outsourcing are to involve sector experts to provide a different perspective or for quality assurance, for specific data collection (e.g. through surveys) and to take over services developed by the Agency that have become too big to handle in-house. In this sense, it can be said that efficiency plays a role when outsourcing decisions are made: work that is faster or cheaper if implemented by an external service provider is considered for outsourcing. However, ENISA staff and management also noted that the Agency received a specific budget from the Commission for procurement and that decisions are made in a way to ensure full use of this budget.

3.2.2.13 Conclusion on effectiveness

Conclusion – Effectiveness

The baseline situation (established based on an evaluation of all EU agencies including ENISA in 2009[52] and an impact assessment of changes to ENISA's mandate in 2010[53]) shows concerns about ENISA's ability to achieve targeted impacts. The main reasons provided were ENISA's limited financial resources and the small size of the Agency. These concerns continued to be relevant in the period 2013-2016, as presented below.

The annual evaluations of ENISA show that the Agency implements its tasks and achieves its set targets. Through this work, ENISA has made a contribution to increased NIS in Europe. However, this contribution is limited by several factors:

- the broad mandate under which a variety of tasks is to be covered,
- the strong influence of Member States when it comes to setting the work programmes,
- the Agency's difficulties in attracting and retaining cybersecurity experts as staff members,
- and the limited visibility of ENISA.

ENISA's activities have made an important contribution to **enhanced cooperation** between Member States and related NIS stakeholders. Community building has been enhanced across Member States and in particular the cooperation between CERTs/CSIRTs has increased. However, the cooperation and exchange between ENISA and the Commission and other EU agencies could still be improved. Furthermore, cooperation with industry stakeholders should be strengthened.

ENISA has contributed to **enhanced capacities** in Member States, most notably in Member States with more limited capabilities and resources in the area of cybersecurity. Important activities have been developed and implemented, such as the Cyber Europe Exercises and trainings for CERTs/CSIRTs. Similarly to its contribution to enhance cooperation, ENISA is not reaching all stakeholders with its capacity building activities. Industry stakeholders could be better involved.

ENISA is limited in the **expertise** it can provide. It makes an important contribution to the CERTs/CSIRTs. Other stakeholders from the Member States, but also the EU institutions and industry representatives, are less convinced by ENISA's expertise. ENISA has not managed to become recognised as a centre of expertise or a reference point for stakeholders. The high reliance on the procurement of external expertise in the implementation of tasks is a consequence of the limited in-house expertise but also the limited resources available.

ENISA has assisted the Member States and the Commission in developing and implementing the **policies** necessary to meet the legal and regulatory requirements of NIS, though the Agency is not consistently being involved by the Commission in all NIS-related activities.

Overall, ENISA has difficulties meeting its objectives. This is linked to the Agency's broad mandate which is not matched by sufficient financial resources. A lot of efforts are being made but they are spread over a wide field of responsibility, therefore ENISA can only have a limited impact on cybersecurity.

---

[52] Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

[53] European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

3.2.3 Efficiency

Efficiency considers the relationship between the resources consumed by an intervention and the changes generated by it (which may be positive or negative).[54] The assessment of the efficiency of ENISA considers the relationship between the resources used by the Agency and the changes generated by its activities. The section also covers the efficiency of ENISA's governance and internal organisational structure. The benchmarking of ENISA with other EU agencies and bodies has been integrated in this section.

The following evaluation questions are covered in the present section:

Table 18: Evaluation questions covered under the efficiency criterion

Main evaluation question	Other evaluation questions
EQ14: To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation? To assess this question, elements relating to internal structure, operation, programming of activities and resources, accountability and controls, etc. will be analysed.	**Retrospective** EQ15: Were the annual budgets of the Agency implemented in an efficient way considering the results achieved? EQ16: Have the resources allocated to the Agency been sufficient for the pursuit of its tasks (input/output analysis)? EQ17: To what extent are the organisational solutions and procedures of ENISA adapted to the work entrusted to it and to the actual workload? Is the planning cycle of the agency (work programme and budget) in line with the objective of achieving efficient results? EQ18: To what extent have ENISA's governance, organisational structure, locations and operations as set in its Regulation and the arrangements related to the location of its offices been conducive to efficiency and to achieving economies of scale? EQ21: To what extent and how have external factors influenced the efficiency of ENISA?

3.2.3.1 ENISA's efficiency considering its governance, organisational structure, procedures, budget and location

EQ14: To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation? To assess this question, elements relating to internal structure, operation, programming of activities and resources, accountability and controls, etc. will be analysed.

EQ17: To what extent are the organisational solutions and procedures of ENISA adapted to the work entrusted to it and to the actual workload? Is the planning cycle of the agency (work programme and budget) in line with the objective of achieving efficient results?

EQ18: To what extent have ENISA's governance, organisational structure, locations and operations as set in its Regulation and the arrangements related to the location of its offices been conducive to efficiency and to achieving economies of scale?

While ENISA's governance structure (with an Executive Board, Management Board and the PSG), management practices and dedicated staff are conducive to the efficient functioning of the Agency, there are a number of areas where further efficiency gains could be made. These relate to the relatively rigid and inflexible planning cycle; the split location between Athens and Heraklion which incurs additional travel costs and costs in terms of ensuring cohesion; its working practices relating to its objective of delivering "expertise" through reports and publications which through a more

---

[54] Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

efficient process of, for example, peer review could be improved in terms of their quality; the need to further modernise and automate given administrative processes; and the need for HR processes to be further formalised to ensure a smoother, quicker process.

ENISA's governance structure is conducive to the efficient functioning of the Agency. The current governance structure was seen as conducive to the efficient functioning of the Agency (i.e. in terms of value for money) by most of the respondents to the survey on ENISA's governance, organisational set-up and working practices (86% or 76 out of 88 respondents) and was judged conducive to this efficiency to a limited or to no extent by only 6% of respondents (5 out of 88). Members of the Management and Executive Boards provided more positive answers than the other groups of respondents: 63% considered the governance structure to be conducive to efficiency "to a high extent". The interviews with staff and ENISA's direct stakeholders also pointed to the fact that ENISA's organisational set-up was adapted to the work it carries out and its workload, enabling it to achieve its objectives in an efficient manner.

Figure 35: Extent of agreement or disagreement with the following statement: The current governance structure with a Management Board, an Executive Board and the PSG is conducive to the efficiency functioning of the Agency (i.e. in terms of value for money)
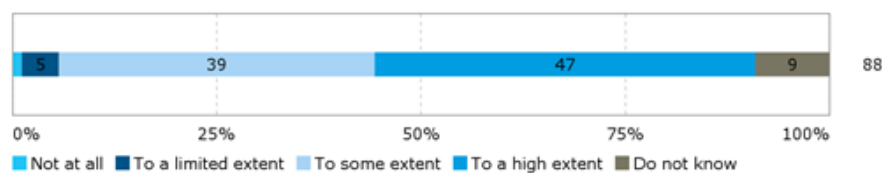
Source: Survey of ENISA staff and direct stakeholders

In particular, the establishment of an Executive Board was judged positively by more than half of respondents (56% or 49 out of 88 respondents) who saw this new board as bringing more efficiency to the functioning of the Management Board to some or to a high extent. A limited number of respondents (10% or 9 out of 88) saw this change as being conducive to more efficiency to a limited extent or not at all - a quarter of NLOs (25%) were of this opinion. In these cases, respondents questioned whether the Executive Board leads to a more efficient functioning of the Management Board, suggesting instead that it only increases the complexity and decreases the transparency of the structure. Interviewees from ENISA staff and direct stakeholders suggested that the Management Board could gain in efficiency by working in smaller, targeted groups that focus on a given topic before feeding back to the plenary (see also section 3.2.2.8). The 2014 and 2015 evaluations supported these findings with reference being made to a clear delineation of responsibilities within the organisation, leading to a good execution of the work.

The comparison with other EU agencies shows that ENISA had a comparatively high number of meetings with its governing bodies. The comparably higher number of Management Board and Executive Board meetings per year for strategic decision making supports the argument made by those respondents who judged that ENISA's governance structure with two boards increased the complexity of the Agency. However, FRA also works with an Executive Board. At the same time, the high number of meetings shows the active engagement of the Management and the Executive Board in the running of the Agency.

Figure 36: Number of Management Board and Executive Board meetings per year for strategic decisions, 2014-2016
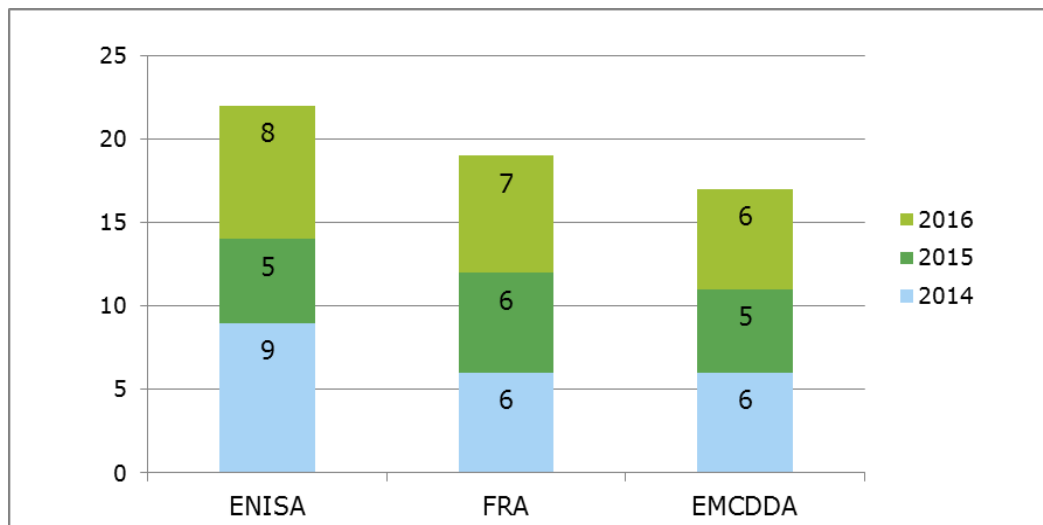
Source: Data gathered through secondary sources and received by ENISA, FRA and EMCDDA.

ENISA's management practices are conducive to creating an efficient organisation. The majority of respondents to the survey of ENISA staff and direct stakeholders (74% or 65 out of 88) saw ENISA's management practices as being conducive to creating an efficient organisation (i.e. in terms of value for money) "to some" or "to a high extent". The interviews with ENISA staff suggested that the fact that many of ENISA's management staff come from the private sector assists in ensuring that the Agency is managed in an efficient way. The number of meetings at management level was also referred to as a means to facilitate the dissemination of information and make management more transparent. However, a total of 18% of respondents (16 out of 88) saw ENISA's management practices as only conducive to such efficiency to a limited or to no extent; it was felt that management and administration overall had too large a role.

Figure 37: Extent of agreement or disagreement with the following statement: ENISA's management practices are conductive to creating an efficient organisation (i.e. in terms of value for money)?
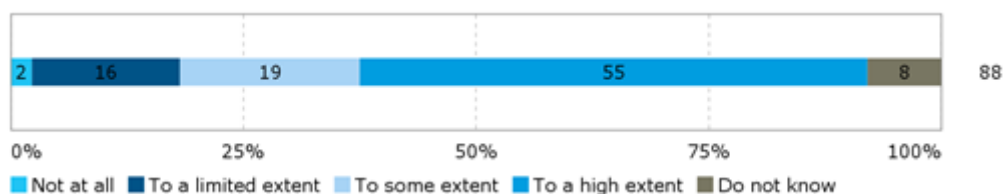
Source: Survey of ENISA staff and direct stakeholders

The planning cycle of the Agency (work programme and budget) is lengthy. The planning process is lengthy and burdensome for management in particular, as detailed in section 3.2.2.5, but was overall deemed necessary and leads to a necessary result. The findings in this same section point to ENISA's work programme being a relatively rigid means of determining work priorities in such a fast-paced area and a lack of continuity in many of its activities from one year to the next due to its aim to cover a wide range of activities and sectors. It can be assumed that increasing the flexibility and continuity of the work programme from one year to the next would therefore likely lead to efficiency gains.

ENISA's working practices are efficient, leading to timely but not necessarily consistently useful, high quality outputs. A large majority of respondents to the survey of ENISA staff and direct stakeholders (84% or 72 out of 86 respondents) saw ENISA's working practices as efficient and making the best use of available resources to some or to a high extent. Some of the tools in place in the Agency are advanced compared to those used by other agencies

and favour efficiency, e.g. the Agency's workflow paperless management system (use of e-signatures). However, nine respondents (16%) saw ENISA's working practices as being conducive to such efficiency only to a limited extent or not at all. ENISA staff members (including management) were slightly more critical of ENISA's working practices than the direct stakeholders with 16% of them regarding them as conducive to efficiency to a limited extent. Reasons provided for such assessments included the level of bureaucracy being too important within ENISA and administrative tasks having to be conducted by operational staff.

Figure 38: Extent of agreement or disagreement with the following statement on ENISA's working practices
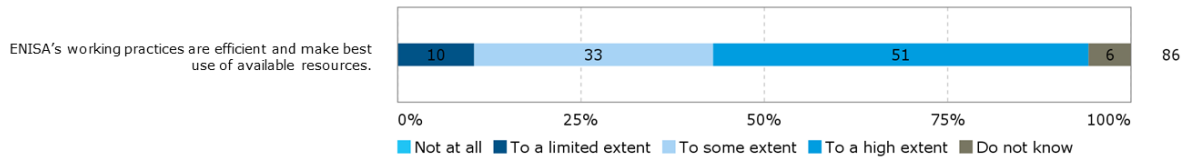
Source: Survey of ENISA staff and direct stakeholders

While ENISA's working practices enable it to produce services in a timely manner, the quality, usefulness and added value of some of its outputs was questioned (see section 3.2.2.7). It was suggested by one interviewee that ENISA could gain in efficiency by procuring less work externally from contractors and drawing more on the expertise of national cybersecurity experts from national authorities, academics and the private sector to assist them in developing reports/publications in-house through a peer review process.

With regards to the internal management systems for planning, follow-up and monitoring the majority of respondents to the survey of ENISA staff and direct stakeholders (70%) saw them as creating value for money "to some" or "to a high extent". This efficiency was viewed to be of "a limited extent" or to exist "not at all" by 10% of respondents. A large number of Management and Executive Board members saw the management systems to be bringing efficiency to some or to a high extent while ENISA staff was on average slightly more likely (16%) to consider the efficiency brought by management systems as being limited or non-existent.

Figure 39: Extent of agreement or disagreement with the following statement regarding ENISA's internal management systems
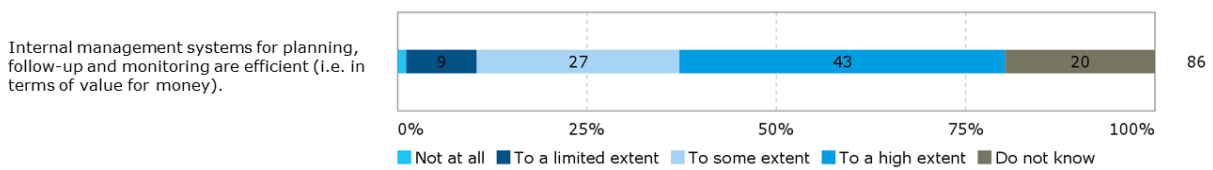
Source: Survey of ENISA staff and direct stakeholders

ENISA's administrative systems are adequate, but could be modernised to increase efficiency. The administrative systems in place to support ENISA's operations were seen by survey respondents as adequate and appropriate to some or to a high extent by a majority of respondents (63% or 54 out of 86 respondents) and to a limited extent or not at all by 21% (18 out of 86). ENISA staff (including management) was more critical than the average in this regard, with 35% of them stating that the administrative systems were adequate and appropriate only to a limited extent or not at all. Those who provided comments on their more negative assessment converged in saying that the administrative systems used were not modern enough and led to a duplication of work; required a lot of manual work to operate, not allowing for automation; and overall impeded the smooth functioning of the Agency.

Figure 40: To what extent do you agree/disagree with the statements below regarding ENISA?

| The administrative systems in place to support ENISA's operations are adequate and appropriate. | 5 | 16 | 35 | 28 | 16 | 86 |

0%   25%   50%   75%   100%

■ Not at all ■ To a limited extent ■ To some extent ■ To a high extent ■ Do not know
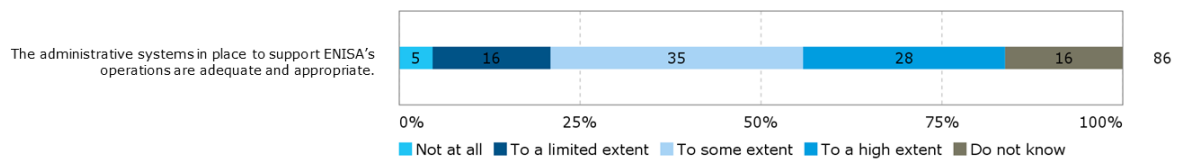
An example of a system referred to in the 2014 evaluation was the MATRIX project management system. Staff book their hours in the system and it provides an overview of resources for each project. MATRIX automatically generates reports for the management on a biweekly basis. However, the system was not considered relevant for generating management information at an operational level, and it was not used actively to steer projects. Instead, in addition to MATRIX, each Core Operations Department (COD) unit used spreadsheets to maintain an overview of projects on a daily basis. These sheets were individual to each unit and varied in content from one unit to another. During the interviews conducted in 2014, ENISA staff indicated that the MATRIX system did not provide for sufficient functions for project management at COD unit level, such as tracking risks and issues. For this reason the spreadsheets were set up, with plans to standardise them in the future.

While the Agency's staff was seen as a source of efficiency, human resource processes and issues are a source of inefficiency. A number of interviewees (ENISA management and Executive Board members) referred to ENISA's motivated, hard-working staff as a key factor to its efficiency. However, ENISA's difficulty in recruiting and retaining staff (see section 3.2.2.8) is a source of inefficiency with significant efforts needing to be put into recruitment by the administrative department. Moreover, inefficiencies in the recruitment process were cited by ENISA staff with references to the lengthy process, the need to ask the same questions of all interviewees making them "unnatural", difficulties in organising interviews when all interview committee members are present, and a lack of follow-up with candidates. It was hoped that the arrival of a new human resources manager in late 2016 would enable the process to become more efficient.

The difficulties in attracting staff are also reflected in the expenditure allocated to recruitment; ENISA dedicates more financial resources to staff recruitment than any of the other agencies and bodies considered under the benchmarking exercise. The figure below shows that 2.5% of ENISA's total expenditure in 2015 was dedicated to staff recruitment; this figure is significantly higher than for agencies and bodies like BEREC, EFCA, CEPOL, EDA and EMCDDA. Despite these efforts, recruitment has not been successful.

Figure 41: Staff recruitment expenditure compared to overall expenditure, 2015
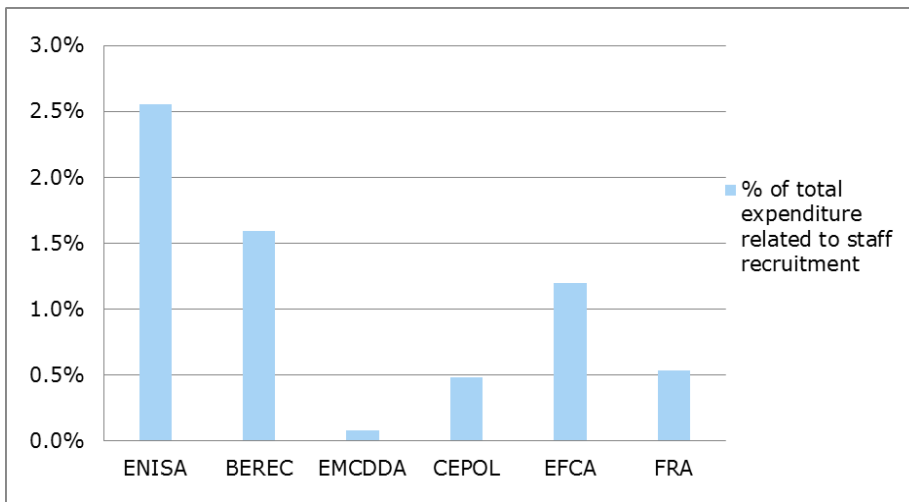
Source: Draft General Budget of the European Union for the financial year 2016 - Working Document Part III Bodies set up by the EU and having legal personality and Public-Private Partnership.

While the setting up of an office in Athens contributed to efficiency gains, the split location of the Agency is not conducive to its efficiency. Moving ENISA's operational units to Athens in 2013 meant an important increase in efficiency. As stated in a Commission cross-cutting study on the decentralised agencies of 2012[55], the overall accessibility of EU agencies affects their efficiency. The study showed that agencies located in very remote places (including ENISA when located in Heraklion) faced difficulties in attracting and retaining staff from the rest of Europe, leading to difficulties in filling the establishment plans with appropriate staff and to geographical imbalances with a high representation of local staff. This issue has been alleviated to a great extent with the move of parts of ENISA to Athens but as shown below, inefficiencies linked to ENISA's location persist.

Among the respondents to the survey of ENISA staff and direct stakeholders, ENISA's current location was judged by 59% (52 out of 88 respondents) as enabling ENISA to conduct its work efficiently (i.e. in terms of value for money) to some or to a high extent. A total of 35% of respondents (31 out of 88) saw it as being conducive to this efficiency to a limited extent or not at all. There was a difference in the opinions of ENISA staff relative to other types of respondents: PSG members, NLOs and Management and Executive Board members saw ENISA's location as only being conducive to its efficiency to a limited extent or not at all (respectively 54%, 50% and 47%) whereas three quarters (75%) of ENISA staff (including management) saw ENISA's location as being conducive to its efficiency to some or to a high extent.

Figure 42: Extent of agreement or disagreement with the following statement: ENISA's location enables it to conduct its work efficiently (i.e. in terms of value for money)
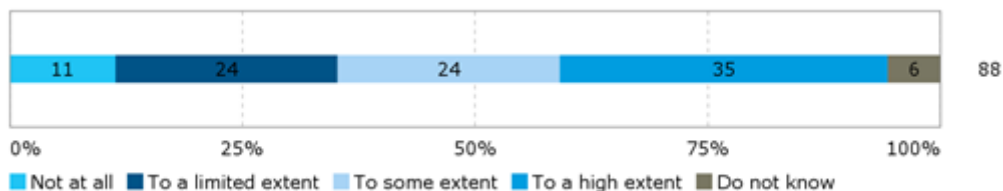
Source: Survey of ENISA staff and direct stakeholders

---

[55] European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No3 – Agencies' seat and role of the host country. Available at: http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_3_sent_to_ep_cons_2010-12-15_en.pdf

The respondents who criticised the efficiency of ENISA's location referred to the costs incurred by travel (direct costs and time commitment), and the duplications of costs related to ENISA's facilities being divided over two locations (between Heraklion and Athens). A few ENISA staff (including management) respondents were critical of the fact that the Agency is divided in two, which it was judged decreased the Agency's efficiency as its incurred additional travel costs, and led to duplications of work from an organisational set-up perspective, e.g. negotiations with landlords and other organisational questions. Inefficiencies in the split location were cited by interviewees as being primarily due to travel costs between Athens and Heraklion and to ensuring cohesion between the two offices, rather than the costs of maintaining an office in two locations. A variety of types of interviewee saw closing the office in Heraklion as a means to increase the Agency's efficiency.

In fact, the Agency itself sees efficiency losses stemming from duplication of services across the two offices. This includes duplication of costs for security and cleaning services as presented in Table 19. The costs listed below for the office in Heraklion represent 24% of ENISA's administrative expenditure in 2016.

Table 19: Annual costs for renting and maintaining two offices

Costs	Athens	Heraklion
Rent of premises	€316,450	€316,444
Security services	€51,000	€47,400
Cleaning services	€24,000	€15,180
Total	€391,450	€379,024

Source: Data provided by ENISA

To this, the staff costs for employees in Heraklion have to be added. According to data provided by ENISA, there were 13 staff members working in Heraklion in 2016, representing a cost of more than 300,000 EUR per year (the number of staff in Heraklion has been reduced to eight in 2017). Similar costs would have to be paid if these staff members were based in Athens. Only the travel costs to Athens of EUR 751 per staff member could be saved.

Table 20: Costs for staff based in Heraklion

Costs	Number of staff	Total
Daily subsistence allowances	13	€83,813
Installation allowances	13	€89,422
Removals	13	€139,000
Travel expenses	13	€751
Total	13	€312,986

Source: Data provided by ENISA

ENISA also assesses that the most important costs stemming from the two offices are related to a loss of productivity due to the separation of the teams and the needs to ensure coordination and across the offices.

ENISA was not seen as achieving economies of scale to the extent that it could. Where ENISA can achieve economies of scale is through its cooperation with other bodies, which as presented in section 3.2.4 is not as effective as it could be. In fact, it was suggested that from a European perspective, ENISA's capabilities and skills could be used more efficiently and economies of scale could be achieved if ENISA is consulted/has a role in any European activity being linked to NIS/Cybersecurity in Europe such as the contractual public-private partnership (cPPP).

3.2.3.2   Implementation of annual budgets

> **EQ15: Were the annual budgets of the Agency implemented in an efficient way considering the results achieved?**
>
> Taking into account the results achieved by the Agency and the limited budget available it can be concluded that ENISA implements its budgets in an efficient way. ENISA makes important achievements in terms of created outputs, such as high numbers of publications and fully uses the allocated funds. The Agency has been able to contribute to its targeted impact (an increased level of NIS in Europe) though could achieve more if more resources were available.
>
> Improvements in budget implementation could be made by reducing the amount of carry-overs from one year to the next and ensuring that the budget is spent evenly within one year. Among the selected sample of EU Agencies, ENISA has the highest share of administrative expenditure.

Over the period 2013 to 2016, ENISA's budget has increased by 16%. The budget of the ENISA comprises a subsidy from the EU budget which constitutes each year to 93% of the Agency's revenue. In addition, revenue stems from rent subsidies from the Government of the Hellenic Republic (which constitutes between 6 and 7% each year), as well as contributions from third countries participating in the work of the Agency (around 1%).

In 2016, the Agency had a budget of EUR 10.5 million. Figure 43 shows the annual increase in ENISA's budget. The overall increase in four years is EUR 1.7m or an increase of 16% relative to the 2013 budget.

Figure 43: ENISA's budget 2013-2016
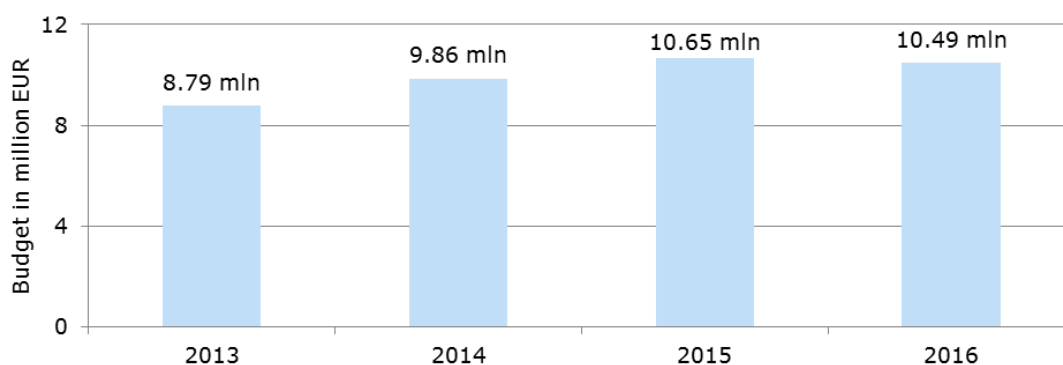
Source: ENISA's Annual Activity Reports (2013, 2014, 2015, 2016)

A comparison to other EU agencies shows that ENISA is among the decentralised agencies with the lowest budget. This is further discussed in section 3.2.3.3 below.

ENISA ensures full budget execution but carry-overs are high; a problem that is encountered by many EU agencies. As shown in Table 21 below, ENISA reached a budget execution rate of its expenditure appropriations of 100% in 2014 and 2015, suggesting high efficiency in the use of its budget. The high payment rate also shows the capacity of the Agency to finalise its annual activities and execute payments as planned and on time. However, the Agency has made use of high carry-overs of committed appropriations from one year to the next.

Table 21: Budget execution of EU subsidy[56]

	2013	2014	2015
Budget execution rate	99.7%	100%	100%
Payment rate on expenditure appropriations	91.3%	85.6%	92.9%
Carry-overs (share of committed appropriations)	13.5%	49%	22%

Source: Court of Auditors reports

The European Court of Auditors commented in its reports on ENISA's high carry-overs. The reports stated that the appropriations primarily concerned administrative expenditure. They were intended for IT equipment and furniture.[57] However, in its 2015 "*Summary of results from the Court's annual audits of the European Agencies and other bodies*" the Court noted that a high level of carry-overs was a frequent comment and concerned many agencies.[58] In 2015, 32 out of 40 assessed agencies were concerned. On average, 36% of committed appropriations for administrative expenditure were carried over. ENISA was thus in 2015 below the average. The execution rates reflect the detailed planning of the EU agencies' budgets and the incentives to ensure full budget execution in order to avoid budget reductions in the following year. This shows that budget implementation could be further improved. ENISA staff and management noted during interviews that there were peaks in spending at the end of each year to ensure that a high budget execution is achieved.

ENISA shows efficiency in the implementation of its different tasks. The annual evaluations of ENISA concluded that processes generally were efficient and a clear delineation of responsibilities within the organisation led to a good execution of the work. ENISA staff and Management Board noted in the interviews that regular follow ups on costs were taking place. Expenditure was assessed to be comparable across the projects. Planning and monitoring of implementation of tasks was reported to be working well. ENISA produces a high number of deliverables and generates good outreach in terms of downloads.

Despite its budget restrictions, the Agency is able to meet its objectives and contributes to some extent to targeted impacts. As shown in sections 3.2.2.1 and 3.2.2.3 ENISA has been effective in implementing its tasks, though not to the extent of a full achievement of targeted objectives and impacts. ENISA is expected to contribute to a long list of tasks and it has proven difficult to contribute to all targeted objectives due to limited financial and human resources. The achievements that are being made show that considerations on the efficient implementation of resources are being made. Along the same lines, the 2015 evaluation indicated that the Agency risks dispersing already scarce resources across too many, too small activities, decreasing the chance of a real impact overall on NIS.

Little potential to increase efficiency was identified. In the annual evaluations of ENISA only small adaptations were suggested to increase efficiency. A main issue raised was the split of ENISA's location which to some extent explains the comparably high share of administrative expenditure of the Agency, as presented in the following section 3.2.3.3. As reported in section 3.2.2.11, monitoring and reporting requirements are generally found to be effective but represent an important burden for staff members.

---

[56] Annual Activity Report 2014

[57] Court of Auditors (2014): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2014 together with the Agency's reply, and Court of Auditors (2016): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2015 together with the Agency's reply

[58] Court of Auditor (2016): Summary of results from the Court's annual audits of the European Agencies and other bodies for the financial year 2015

3.2.3.3   Adequacy of allocated resources

EQ16: Have the resources allocated to the Agency been sufficient for the pursuit of its tasks (input/output analysis)?
Compared to other EU agencies ENISA has a small budget and a low number of staff. The share of CAs among the staff is comparably high. There is concern among ENISA's stakeholders that the Agency does not have sufficient resources to complete its tasks to its full potential; issues relating to the degree to which it is reaching its targeted objectives and impacts are presented in section 3.2.2.1. In particular, more staff is needed. As a consequence of the limited resources, ENISA's Management Board has to prioritise tasks for the Agency. ENISA relies on the dedication of staff members to ensure the implementation of tasks despite insufficient resources.

ENISA works with a comparably low budget and a low number of staff. In 2016, ENISA had 69 staff members of which 24 were CAs. Staff increased by 14% between 2013 and 2016. At the same time, the share of CAs among staff increased from 22% to 35%. To some extent the increasing employment of CAs can be considered a cost-saving measure. The annual evaluations of ENISA's activities noted that this would also represent a risk of increasing staff turnover and making positions less attractive, thus increasing the recruitment problem.

In fact, ENISA has one of the lowest budgets and levels of human resources compared to all EU agencies**.** The figure below positions ENISA among 40 agencies covered by the European Court of Auditors report on agencies in 2016. The figure shows that ENISA is among the agencies with the lowest budget and lowest number of staff. However, the figure also shows that comparably small agencies tend to have low staff numbers in relation to their budget when compared with the trend line.

Figure 44: Comparison of EU agencies based on staff and budget, 2017
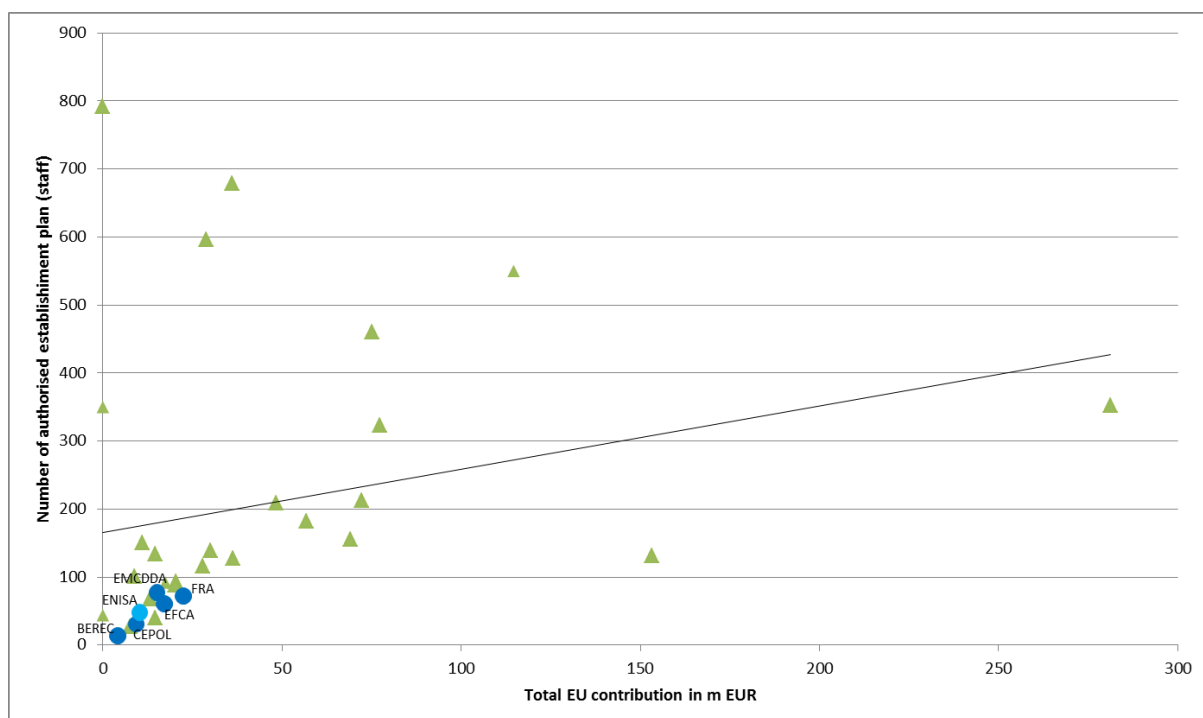
Source: Ramboll Management Consulting, based on Draft General Budget of the EU for the financial year 2018 - Working Document Part III - Bodies set up by having legal personality and Public-Private Partnership (COM(2017) 400 - June 2017)

The share of administrative expenditure of ENISA is higher than that of other EU agencies considered in the benchmarking exercise. For example, in 2015 CEPOL, with a total budget similar to ENISA's but slightly lower staff numbers, used less than 6% of its budget as administrative expenditure. EFCA, even more similar in its total budget and staff numbers to

ENISA, used 12.42% of its budget for administrative expenditure in the same year, while ENISA's administrative expenditure amounted to 14.8% of its total budget.

Figure 45: Distribution of commitment appropriations between staff, administrative and operational expenditure, 2015
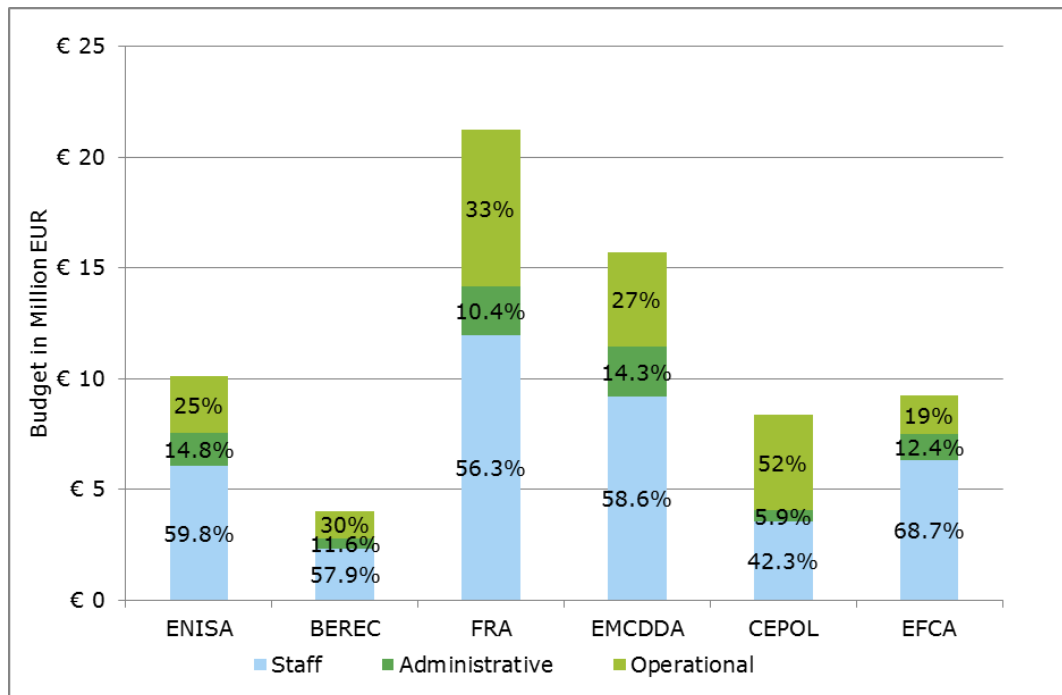
Source: presentation by Ramboll, data from European Commission: Draft General Budget of the European Union for the

financial year 2016 - Working Document Part III

When comparing the distribution of staff between operational and administrative roles, as presented in Figure 46 below, it shows that ENISA has with 21% a very similar share of administrative staff as EMCDDA. However, FRA has a share of administrative staff of only 17%. Considering the much higher budget of FRA, this suggests that there are some economies of scale for larger agencies when it comes to the execution of administrative tasks. ENISA, as a small agency, cannot benefit from these.

Figure 46: Staff distribution between operational and administrative staff for ENISA, FRA and EMCDDA, 2015
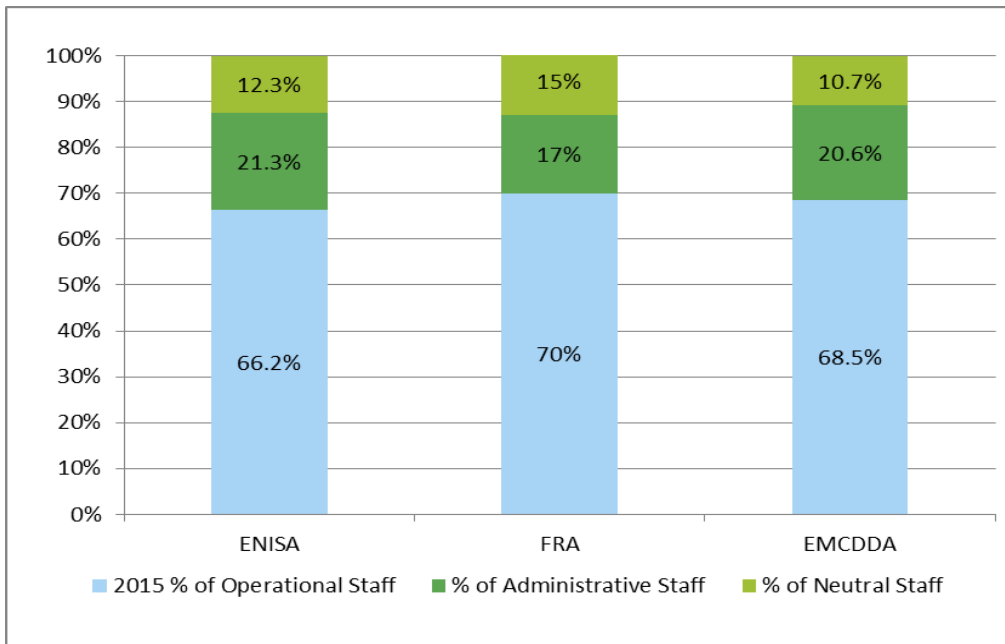
Source: Data gathered through secondary sources and received by ENISA, FRA and EMCDDA.

There is concern among ENISA's stakeholders that the Agency does not have sufficient resources to meet the challenges in the cybersecurity area. Direct stakeholders, such as the Member States, see that ENISA is not able to respond to all their needs. This is reflected in the process of setting ENISA's annual work programme where it is not possible to include requests from all members of the Management Board. More external stakeholders, such as other EU agencies, stressed that ENISA is also affected in its day-to-day work by its limited resources, for example in it being absent from key cybersecurity events. In the end, as shown in section 3.2.2, ENISA has difficulties to meet its objectives due to an important scope of its mandate which is matched with only a limited number of resources.

Moreover, among the open public consultation respondents, 58% (38 out of 65) considered the size of the agency with 84 staff members to be partially or completely inadequate. There were no notable differences between the different respondent groups.

Figure 47: Adequacy of the size of the Agency for the work entrusted to it (n=65)
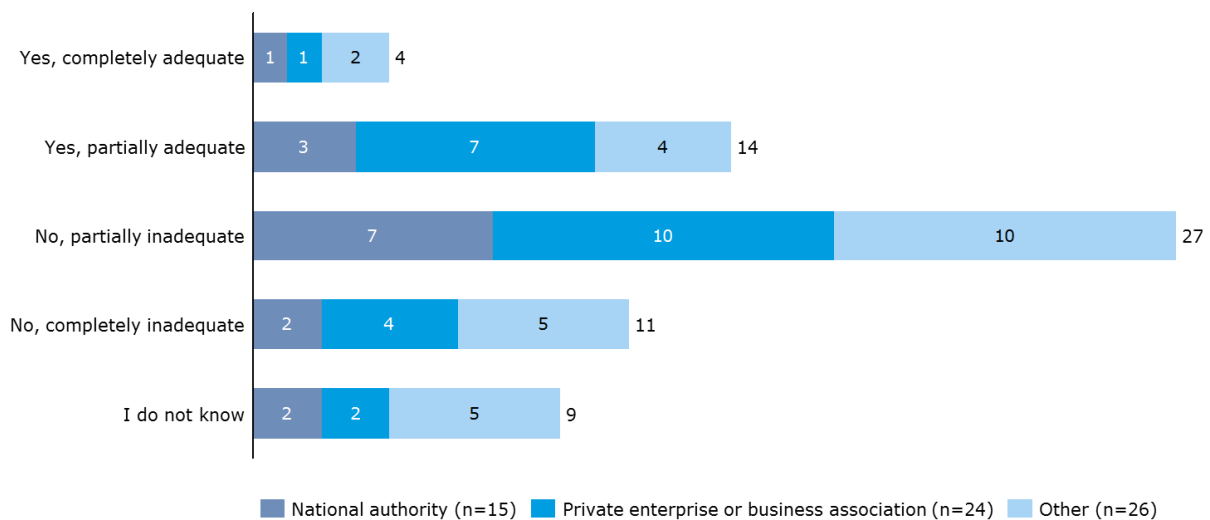
Source: Open public consultation

Please also refer to the findings on ENISA's human resources in section 3.2.2.8.

The insufficient human and financial resources require a lot of dedication from the staff to complete their work and a strict prioritisation of tasks in the work programme. ENISA is not able to respond to all needs of its stakeholders but has to focus on the most urgent ones. The Management Board has to set priorities within the tasks ENISA is supposed to fulfil based on its mandate.

The limited resources represent a burden on staff who take on additional work. ENISA's management and Management Board confirmed that ENISA was highly dependent on the dedication and willingness of staff to work overtime in order to implement the work programme and meet expected standards. The small budget also limits ENISA's visibility. The main concern is to implement the Work Programme rather than build relationships with the stakeholders and, for example, visit all Member States at least once a year or follow up on the use of publications to gain insights on stakeholder requests for future work.

3.2.3.4   Influence of external factors on efficiency

EQ21: To what extent and how have external factors influenced the efficiency of ENISA?
Evidence shows that ENISA's efficiency is negatively influenced by limited exchanges with the Commission on its plans for the Agency, and limited exchange and cooperation with other EU bodies.

Limited communication of the Commission when deciding on (new) tasks for ENISA has a negative impact on the Agency's efficiency. The findings from interviews and the annual evaluations of ENISA suggest that there is some concern that the Commission does not sufficiently exchange with the Agency on the feasibility of implementing additional tasks when planning the allocation of new responsibilities. One example given was the role of ENISA under the NIS Directive. ENISA's staff and management reported that they were not sufficiently able to comment on the feasibility of the tasks foreseen in the legislative text, as developed by the Commission, the European Parliament and the Council. Inefficiencies are created where the Agency then needs to adapt its Work Programme and drop tasks on which work was already planned or even started.

The fragmentation of cybersecurity across different European Commission DGs, EU bodies and agencies creates inefficiencies where information is not shared or work is duplicated. Besides ENISA, a number of other EU agencies and bodies (including CERT-EU and Europol's EC3) are active in different fields relating to cybersecurity. Also a number of European Commission DGs are touching in their work upon cybersecurity issues. These are for example beside DG Connect, DG Energy when covering security of energy grids or the DG for Economic and Financial Affairs when considering security of online banking. ENISA staff and management, as well as other interviewed stakeholders, expressed concern that inefficiencies were caused by two or more organisations working on the same topic and insufficiently sharing information about their work with one another. A further assessment of ENISA's cooperation with EU bodies and potential duplication of efforts is presented in section 3.2.4.

3.2.3.5   Conclusion on efficiency

Conclusion – Efficiency

The baseline situation, (established based on an evaluation of all EU agencies including ENISA in 2009[59] and an impact assessment of changes to ENISA's mandate in 2010[60]) points to ENISA being one of the smallest agencies in the EU. In 2009, ENISA had 57 staff members and a budget of EUR 8 million. Together with its location in Heraklion, this factor was considered to impact on its efficiency. Since then, this evaluation shows that ENISA has slightly grown in size but the resources allocated to it are still not considered to be sufficient. The move of ENISA's operational staff to Athens increased ENISA's efficiency.

ENISA demonstrates efficiency in the implementation of its tasks. ENISA has among the lowest budgets and levels of human resources compared to other EU agencies. In order to complete the various tasks set out in its mandate, ENISA has to be very efficient in the implementation of its budget and carefully consider where resources and working hours can be spent. The Agency develops a high number of publications every year and implements many other activities. Despite its small budget, the Agency has been able to contribute to targeted objectives and impacts, showing efficiency in the use of its budget.

The assessment of the distribution of financial resources showed that while ENISA has a similar budget execution rate, relative to the other agencies reviewed as part of the benchmarking exercise. Its administrative expenditure was higher. The Agency has to fulfil a number of administrative requirements as set by the Commission. These requirements are the same for all EU agencies but weigh more heavily on smaller agencies.

One of the main challenges to the Agency's efficiency relates to ENISA's difficulties in recruiting and retaining staff, also compared to other agencies and bodies considered as part of the benchmarking exercise. Despite allocating the highest level of expenditure to staff recruitment in comparative terms, posts are not being filled. The data showed that ENISA's ability to maintain staff gradually decreased over the years, whereas other agencies such as FRA and ECMDDA maintained roughly the same number of staff.

ENISA's efficiency is further limited by its split location: having two offices means that the Agency has to implement additional efforts to ensure coordination between the offices and bear the extra travel costs.

3.2.4   Coherence

The evaluation criterion coherence assesses how well or not different actions work together.[61] For this evaluation, the focus has been set on the external coherence of ENISA's work with other EU Agencies and institutions, as well as with the Member States. This section also integrates the positioning exercise, under which the scope of services and products offered by ENISA has been compared to that of other EU agencies and bodies, as well as to Member States' cybersecurity organisations. The complete data of the positioning exercise is presented in Appendix 4.

---

[59] Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

[60] European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

[61] Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

Table 22: Evaluation questions covered under the coherence criterion

Main evaluation question	Other evaluation questions
EQ24: To what extent are ENISA activities coherent with the policies, strategy documents and activities of other stakeholders?	**Retrospective** EQ9: How does ENISA compare to the other EU and national bodies offering similar services in relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency? EQ10: To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements? EQ22: To what extent is ENISA acting in cooperation with *the European Commission and other EU bodies*, to ensure complementarity and avoid duplication of efforts? EQ23: To what extent is ENISA acting in cooperation with the *Member States* to ensure complementarity and avoid duplication of efforts? EQ25: Are the procedures put in place effective to ensure that ENISA's cooperation activities are coherent with the policies and activities of its stakeholders? EQ26: What are the risks/sources of overlaps/conflict of interests?

3.2.4.1 ENISA's cooperation with the European Commission and other EU bodies

EQ22: To what extent is ENISA acting in cooperation with the European Commission and other EU bodies to ensure complementarity and avoid duplication of efforts?
ENISA's activities were found to be generally coherent with the activities of the European Commission and other EU bodies. Some cooperation is taking place and leads to complementarity. Nevertheless, the cooperation between ENISA and the different Commission DGs could be increased. It seems as if so far there is no reflex to involve ENISA in all Commission activities concerning cybersecurity. With some EU bodies, including the Commission's DG Energy and EC3, ENISA is successfully cooperating by developing and implementing common activities.

ENISA's activities were identified as being coherent with the policies and activities of its stakeholders. Almost all respondents (94%) to the survey of ENISA staff and direct stakeholders regarded ENISA's activities as being coherent with the policies and activities of its stakeholders to some or to a high extent.

Figure 48: Extent of agreement or disagreement with the following statement on the coherence of ENISA's activities
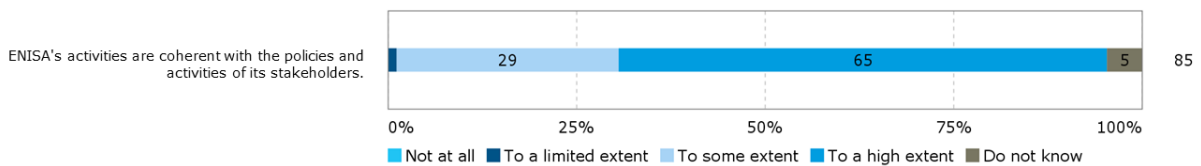
Source: Survey of ENISA staff and direct stakeholders

The coherence of ENISA's activities with EU political priorities was also confirmed during interviews as outlined in 3.2.1.2.

There were diverging assessments of cooperation between ENISA and the European Commission and other agencies but a desire for more cooperation was expressed. The annual evaluations of ENISA's activities in 2014 and 2015 concluded that the Agency actively pursued cooperation with other relevant EU stakeholders. Many interviewees across all stakeholder groups noted that coordination efforts were high and systematic exchanges took place but were limited by constraints in resources on ENISA's side. In contrast, even more interviewees, including several Commission representatives thought that cooperation between ENISA and the Commission

could be further improved. The location of ENISA was cited as one source for this lack of coordination by several members of the Commission. No overlaps or conflicts of interest were identified between ENISA and the Commission due to lacking cooperation but stakeholders saw room for improvement to allow for more coordinated planning of ENISA's activities. From the perspective of ENISA's staff and management, as well as the Management Board, a desire was expressed that the different Commission DGs should rely more on ENISA's services and systematically involve the Agency when dealing with cybersecurity issues. Cooperation between the DG JRC and ENISA was generally assessed to be limited to specific projects. The DG JRC conducts research on request by DG CNECT, and where ENISA covers the same issue some degree of coordination is implemented to avoid duplication of work. However, there was no evidence of more systematic coordination to ensure synergies.

The cooperation with other EU bodies and agencies could be further improved to enhance synergies. There are some efforts by ENISA to cooperate with other EU bodies like Europol's EC3. EC3 is represented in ENISA's PSG and the organisations have cooperated in the past on some activities, like the organisation of workshops aimed at defining a common taxonomy between CERTs/CSIRTs and law enforcement.[62] However, the European landscape of cybersecurity remains fragmented with many actors covering specific fields and without an organisation acting as an umbrella for these different activities guiding the distribution of tasks. Duplications of efforts easily arise, as stakeholders are not fully aware of all activities of the different organisations active in the field of cybersecurity. A detailed assessment of overlaps and complementarities between ENISA, CERT-EU, the DG JRC and EC3 is presented in section 3.2.4.3. In particular, the positioning of ENISA relative to CERT-EU showed a risk for overlap in certain areas.

3.2.4.2   ENISA's cooperation with the Member States

> **EQ23: To what extent is ENISA acting in cooperation with the Member States to ensure complementarity and avoid duplication of efforts?**
> In general, ENISA's activities are coherent with the activities of the Member States. There is a strong coherence and there are synergies between ENISA's activities and those of the national CERTs/CSIRTs. ENISA is duplicating the efforts of some of the Member States' national cybersecurity authorities. This applies mainly to Member States with a lot of experience and resources in cybersecurity, whereas Member States with fewer resources and capacities are more reliant on ENISA's support.

Overall, there is a good level of cooperation between Member States and ENISA which ensures complementarity and avoids a duplication of efforts. CERT/CSIRT stakeholders were asked in a survey to assess the extent to which the activities conducted by ENISA to support CERTs/CSIRTs over the 2013-2016 period were coherent with and complementary to (i.e. not overlapping or duplicating) what CERTs/CSIRTs were doing. For each of ENISA's activities, a large majority of respondents saw a high or some coherence with CSIRT's activities. The three most coherent activities cited were "organising and managing large-scale cybersecurity measures", "supporting cooperation among CERTs/CSIRTs within the CERT/CSRIT network" and "organising workshops and conferences". The activity that was seen as least complementary with CERTs/CSIRTs' activities was "supporting the collaboration between CERTs/CSIRTs and law enforcement communities, in responding to recent policy and technical developments in this area". Also "creating tools and best practices" and "developing training methodologies" were considered to be less complementary.

---

[62] https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop

Figure 49: Extent to which ENISA's activities towards CERTs/CSIRTs were coherent with and complementary to (i.e. not overlapping or duplicating) what CERTs/CSIRTs were doing
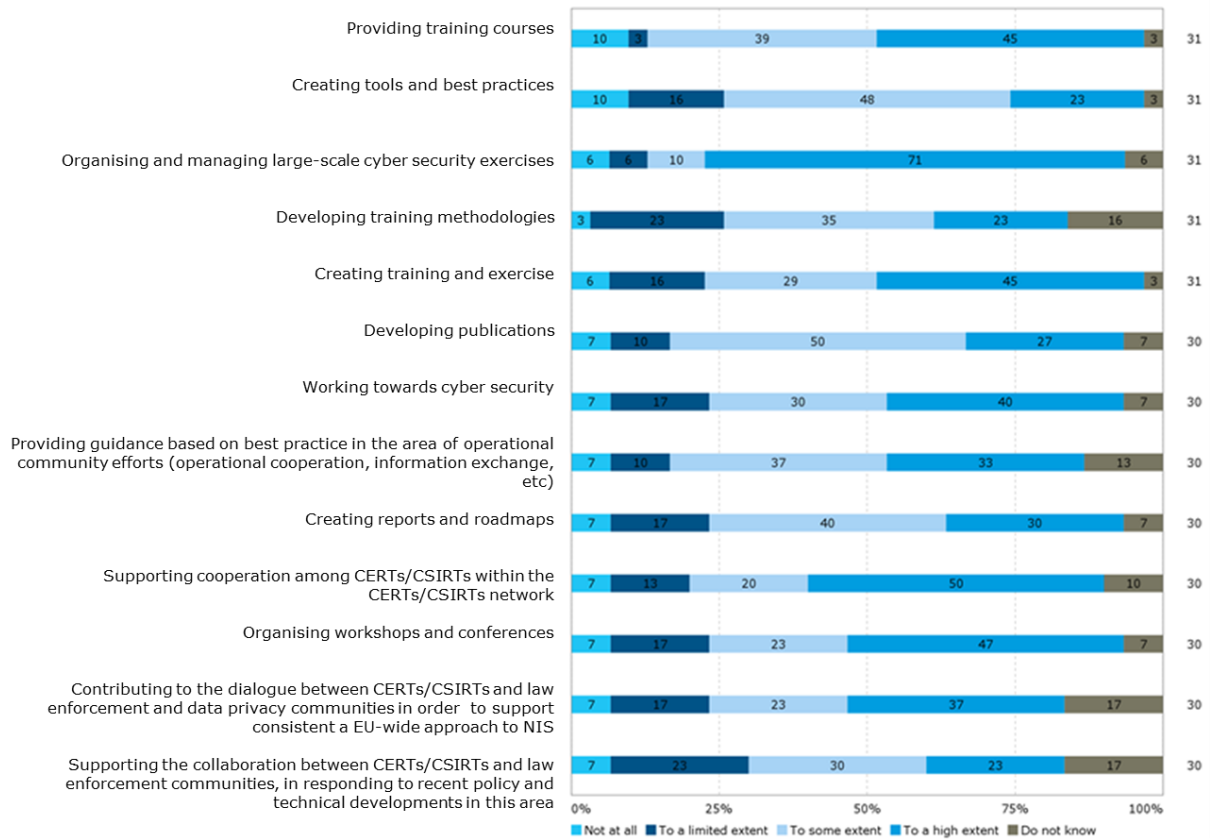
Source: CERT/CSIRT survey

To some extent duplication of efforts can be observed between Member States with strong expertise in cybersecurity and ENISA. The positioning exercise showed a duplication of efforts between ENISA and these Member States, as can be seen in the analysis of the services of ANSSI, NCSC and INCIBE (see section 3.2.4.3). The same activities are however benefiting Member States which do not have the same capacities and resources as their larger neighbours.

3.2.4.3   Positioning of ENISA relative to other EU bodies and national organisations active in the NIS area

EQ9: How does ENISA compare to the other EU and national bodies offering similar services in relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency?

ENISA is able to some extent to respond to the cybersecurity needs of its constituency. There are however certain needs being covered by other EU bodies or within the Member States. Considering the growth in relevance of activities in promoting NIS in the past few years, there is room for a lot of different actors to cover the various thematic fields and the different needs of a growing group of stakeholders concerned by NIS. ENISA is not able to respond to all these needs but meets stakeholders' expectations in specific areas, such as the implementation of exercises and fostering cooperation between the Member States.

In comparison to CERT-EU, ENISA is perceived as being less flexible in responding to unforeseen needs but is valued for its independent point of view. In those Member States where resources and capacities in the area of cybersecurity are high, national sources of information are preferred over ENISA's reports as they come in national language and are perceived to be more tailored to given

Member States' circumstances. However, for stakeholders in Member States with fewer resources being invested in cybersecurity, ENISA represents a valued source of information and provider of services.

As presented in section 3.2.1.3, most of ENISA's stakeholders do not expect ENISA to cover digital privacy needs.

EQ10: To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements?

ENISA was found to be only partially effective in the achievement of targeted results, primarily due to its limited resources and the broad mandate to be covered. Compared to other current EU bodies active in the area of NIS, ENISA seems to be more restricted in its capacity to effectively achieve results. For example, CERT-EU has for some stakeholders become the preferred source of expertise when setting up a CERT or when searching for information on threats even though its mandate points to it being a body at the service of EU institutions, agencies and bodies.

Compared to Member States' organisations, ENISA provides value in particular where it brings together stakeholders from across the EU and representing different sectors. However, the degree to which ENISA has been effective at achieving its intended results varies from one Member State to another. In general terms, the cybersecurity bodies of more experienced Member States are effective in policy development, capacity building and the provision of expertise, while in Member States with less capacity and expertise, ENISA's activities lead to better results.

EQ26: What are the risks/sources of overlap/conflict of interests?

The evaluation identified risks of overlap between ENISA and CERT-EU, specifically in the area of fostering cooperation across the Member States and the advice provided to CERTs/CSIRTs. CERT-EU is implementing activities that do not only target its constituents (i.e. the EU institutions, agencies and bodies) but also those of ENISA. In the provision of analysis of risks and threats and training activities, CERT-EU has become a relevant source for national public and private stakeholders. No overlaps were identified between ENISA and EC3. The DG JRC and ENISA cover similar topics and have published reports with comparable content, but the DG JRC implements research and testing in the field of cybersecurity which is something that does not fall within the mandate of ENISA. There is no direct coordination of the work between ENISA and the DG JRC which gives rise to a potential for a duplication of efforts. However, DG CNECT coordinates the distribution of work, thereby reducing this potential for a duplication of efforts.

Member States with strong capacities in cybersecurity tend to implement similar activities as ENISA. While these are focussed on the national context and produced in the national language, there is some doubt whether ENISA actually needs to provide similar services. In some cases the EU level perspective can add another useful layer of information and exchange, but in other cases it is not clear whether ENISA adds any value. This however applies only to Member States with strong capacities and experience in cybersecurity. Member States with fewer resources rely on ENISA's services.

This section of the report is based on the positioning exercise which evaluated how ENISA is positioned vis-à-vis a sample of other EU and national bodies working on cybersecurity and digital privacy on the basis of the services offered and the needs expressed by the Agency's stakeholders. The organisations covered in the positioning exercise are CERT-EU, EC3, the DG JRC, the French ANSSI, the Spanish INCIBE and the Dutch NCSC. ENISA's activities have been mapped across the Agency's four tasks: enhancing cooperation, develop and maintain a high level of expertise,

enhancing capacity building and developing and implementing policies. Sub-categories of these have been developed to understand more specific tasks that have been implemented. The complete mapping of ENISA's services and the detailed assessment of the services of the other organisations under review is attached in Appendix 4. The methodology applied for this exercise is described in section 2.3.

ENISA responds to some extent to the needs of its constituency by providing expertise, enhancing capacity and cooperation, and supporting the development and implementation of policy. As outlined in section 3.2.1, ENISA's focus is set on cybersecurity needs. There is less demand for support in the digital privacy area. The findings of the evaluation also show that ENISA is not able to meet all the needs of its stakeholders, primarily due to its limited resources.

Respondents to the open public consultation were asked to assess whether the activities of ENISA were coherent with the policies and activities of their own organisation. 83% of respondents (54 out of 65) considered ENISA's activities to be to a large or to some extent coherent (e.g. take into account, do not overlap, do not conflict with) with the policies and activities of their organisation. This was the case for respondents across all categories.

Figure 50: Extent to which ENISA's activities are coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of respondent's organisation, (n=65)
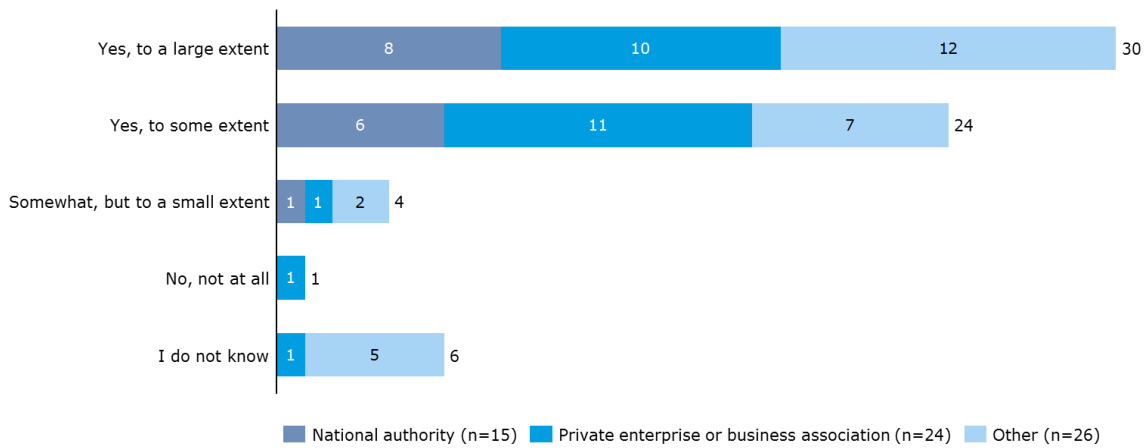
Source: Open public consultation

Respondents were further asked whether they considered ENISA's activities to be coherent with the policies and activities of its stakeholders, including other EU agencies and bodies. In total, 68% of respondents (44) considered ENISA's activities to be largely or to some extent coherent. This is comparably lower than for the coherence with respondents' own organisation. Also the share of respondents considering ENISA's activities to be coherent to a large extent was lower for this second question (46% against 23%).

Figure 51: Extent to which ENISA's activities are coherent e.g. take into account, do not overlap, do not conflict, with the policies and activities of its stakeholders, (n=65)
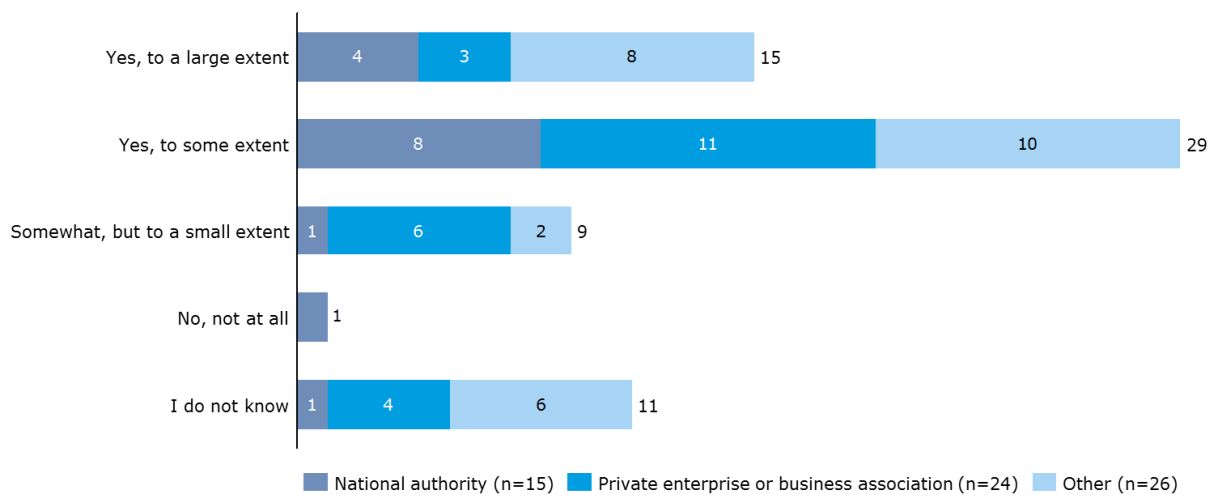
Source: Open public consultation

Respondents who indicated in one or both of the questions that ENISA's activities were coherent to only a small extent or not at all, were asked to provide further explanations. Those that considered ENISA's activities not to be coherent with their own organisation's activities mainly referred to issues with ENISA being up-to-date with the latest developments with regard to legislation or technical evolution. Respondents that saw ENISA's activities to be coherent only to a small extent or not at all with policies and activities of other stakeholders mentioned a lack of clear distinction between the roles of ENISA and CERT-EU. Respondents also mentioned potential overlaps with other organisations (including the cybersecurity bodies of the Member States and the European Cyber Security Organisation).

EU bodies

ENISA and CERT-EU

A comparison between the activities of ENISA and those of CERT-EU shows that there are some complementarities but also a risk of overlap.[63] CERT-EU is the Computer Emergency Response Team for the EU institutions, agencies and bodies, established in 2012. The team is made up of IT security experts from the main EU institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, and the Economic and Social Committee).[64] Its Steering Board is composed of one member of senior management designated by each of the EU institutions or bodies, the Commission may designate up to two further members. EU agencies are represented by ENISA.[65] CERT-EU's mission is to support the EU institutions, agencies and bodies to protect themselves against cyber-attacks. This is done by providing information on threats, vulnerabilities and protection measures, by disseminating information to its constituents in case of an attack and to ensure coordination of response.[66] The activities also include the delivery of extended security services, such as

---

[63] According to the Commission's Better Regulation Guidelines, "complementarity" means that similar initiatives (of different organisations) contribute to the same overall objective and approach it from different perspectives. "Overlap" signifies that several interventions are delivering the same effects for the same people and at the same time.

[64] https://cert.europa.eu/cert/plainedition/en/cert_about.html

[65] Council of the European Union (2014): Information note - Recommendations by the inter-institutional Steering Board of the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) on the future mandate, governance, organisational setup, staffing and funding of CERT-EU. Brussels, 9 September 2014 – document number 12992/14

[66] CERT-EU (2013): RFC 2350

penetration testing and vulnerability assessment. The scope of CERT-EU's activities thus covers prevention, detection, response and recovery.

In general, the services provided by CERT-EU to the EU institutions, bodies and agencies are complementary to the work undertaken by ENISA to coordinate and promote cooperation at EU level among the Member States. The work of both bodies touches upon the field of prevention, for example, through the preparation of regular threat analysis reports and knowledge and methodology enhancement. In the field of threat analysis, the two bodies complement one another as CERT-EU provides daily, current information, while ENISA's Threat Landscape reports are published on an annual basis, thus providing more in-depth assessments. In theory, the targeted audience of the two bodies differs. However, CERT-EU's mandate includes a provision stating that the body may undertake any activities going beyond its mandate with the prior approval of the Steering Board.[67] In practice, CERT-EU has become a reference point for technical advice for organisations interested in building up a CERT. CERT-EU also acts as a point of exchange between the Member States on cybersecurity issues. The body is aware of threats and issues in the different Member States and to some extent shares this information with the other Member States. Here CERT-EU enhances capacity and cooperation beyond its core stakeholders and implements activities that would also be within the scope of ENISA's mandate. CERT-EU responds to a need that ENISA has not been able to fill due to limited financial and human resources (see section 3.2.3.3).

A high number of interviewees from different stakeholder groups expressed concern about this and saw a risk of overlap in the activities of the two bodies. For example, CERT-EU's website provides a news monitor on vulnerabilities, threats and incidents, but also on the activities of different CERTs/CSIRTs. Another example of CERT-EU's activities targeted at national CERTs/CSIRTs were workshops on Malware Information Sharing Platforms. The described activities do not represent an overlap with ENISA's activities because the Agency does not provide the same services at the moment. However, they fall within the remit of ENISA's mandate and there is a risk of duplication of work if both organisations were to provide similar services to national CERTs/CSIRTs.

CERT-EU seems to be closing a gap in services that are needed by ENISA's constituents, but that the Agency, as a decentralised, neutral source, cannot provide due to its limited resources. According to some of the interviewed stakeholders (direct stakeholders), CERT-EU is being contacted by stakeholders beyond its constituents for specific advice, for example on creating a CERT. CERT-EU is considered to be quicker in providing responses to such specific requests. CERT-EU also has the advantage of being located in Brussels which a few interviewees suggested was one of the reasons why CERT-EU was considered to be more accessible by CERTs/CSIRTs but also the broader stakeholder community. While this study showed that ENISA's lack of visibility is not only due to the perceived distance of its location to Brussels, these stakeholder views show that there is some importance placed on the Agency's location when comparing it to other bodies or agencies. As CERT-EU is an inter-institutional body and not a decentralised agency it can more easily ensure direct cooperation with the different DGs of the Commission. However, as a decentralised agency, ENISA is recognised by the Member States and the private sector as a neutral and independent source of information. This was reflected in the open public consultation, where national authorities very frequently and respondents from the private sector frequently indicated "the products and services provide information that is independent and neutral" as a reason for using ENISA's products and services. Interviewees from ENISA's staff and Management Board reported that with additional resources some of the services provided by CERT-EU could also be implemented by ENISA. However, as presented in section 3.2.3.3, with limited staff available ENISA needs to focus on given tasks in order to be able to implement its work programme.

---

[67] Council of the European Union (2015): Information note - CERT-EU mandate, service catalogue and information sharing and exchange framework. 3 March 2015 – document number 6738/15

ENISA and EC3

Little to no overlap was identified between ENISA and Europol's EC3; the two organisations seem to cooperate well. The European Cybercrime Centre was set up by Europol in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime.[68] The organisation implements capacity building and policy development and implementation in the area of cybercrime. There are some topics in which the activities of ENISA can touch upon what EC3 does. For example, EC3 works on the development of a common taxonomy for CERTs/CSIRTs to facilitate cooperation and implements training to authorities in Member States. The evaluation findings show that in these cases ENISA and EC3 tend to work together rather than creating duplications.

While there is some institutionalised coordination between ENISA and EC3, day-to-day cooperation could be further improved. ENISA sits on the Steering Board of EC3. In turn, EC3 is represented in ENISA's PSG. This allows for coordination of the organisations' work. However, interviewees suggested that there could be even more coordination to avoid duplication of efforts on a daily level. While the reports of EC3 take a cybercrime perspective on topics that might be covered by ENISA, ENISA staff and management suggested that this does not fully avoid any overlaps.

ENISA and the DG JRC

Generally, there is complementarity between ENISA's work and that undertaken by the DG JRC Science Hub as the organisations vary in the stakeholders they target and approach issues from different perspectives. The DG JRC is the Commission's science and knowledge service, carrying out research in order to provide independent advice and support to EU policy. The DG JRC conducts research in the NIS area on issues that are very similar to what ENISA covers. However, as a research centre, the DG JRC implements research and testing which in this form is not provided by ENISA. The DG JRC's activities primarily come in the form of a contribution to the Commission's work and are in this sense complementary to ENISA's work which is more targeted at Member States and a broader stakeholder group. For example, the DG JRC published a risk assessment of cloud computing for citizens in 2012.[69] ENISA published a study on the same topic in 2017, but provided an overview of different components to protect data in the cloud and discussed challenges to privacy as well as security.[70] With an overview of different benefits and weaknesses, ENISA's publication was more directly targeted to the Agency's stakeholders.

Where the DG JRC targets stakeholders beyond the Commission with its work, the organisation complements ENISA's work by taking different angles. Through the ITIS project, the DG JRC provides news bulletins on vulnerabilities and threats for the energy sector in the EU and prepares reports on foresight for emerging threats. This complements ENISA's annual threat landscape reports which cover a broader range of sectors. In the past, the two organisations have cooperated in the organisation of exercises such as the first Pan-European CIIP exercise in 2010.

---

[68] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[69] JRC (2012): Will the cloud make the citizen more vulnerable? Risk and vulnerability assessment in times of cloud computing. Available at: https://ec.europa.eu/jrc/en/publication/contributions-conferences/will-cloud-make-citizen-more-vulnerable-risk-and-vulnerability-assessment-times-cloud-computing

[70] ENISA (2017): Privacy and Security in Personal Data Clouds. Available at; https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds

There is a risk of duplication of efforts between ENISA and the DG JRC as both organisations cover very similar issues and no systematic coordination is in place. There are a number of topics on which both bodies are conducting research and producing publications. This includes the threat analysis, as mentioned previously, but also the identification of good practices and recommendations as well as knowledge and methodology enhancement. For example, ENISA published a study on approaches to risk assessment for cybersecurity in the Member States in 2013.[71] This study had a strong focus on the protection of critical infrastructures. In 2015, the DG JRC published a report entitled "Risk assessment methodologies for critical infrastructure protection"[72] also assessing Member States' practices. With such similar focus of their work, there is a clear need to ensure coordination or at least some awareness of what is being done in each organisation to avoid duplication of work. During the interviews ENISA management noted that there was no formal coordination process set up between ENISA and the DG JRC, but that it was rather DG CNECT that guided the scope of the work of DG JRC in the cybersecurity area and thus looking to identify any potential overlap with ENISA's work. While there seems to be well functioning ad-hoc/informal coordination, whereby the DG JRC and ENISA are aware that they are working on similar issues, a risk of duplication of efforts remains if this awareness is not systematically ensured.

National organisations

ENISA's activities have been further compared to those of national bodies. Organisations from Member States with rather developed experience and capacities in the field of NIS have been selected for this purpose.

The Spanish INCIBE implements similar activities to ENISA in the area of expertise, policy development, capacity building and cooperation; in most fields they cooperate with and complement ENISA, there is however some potential overlap. The Spanish National Cybersecurity Institute is a subsidiary of the Secretary of State for the Information Society and Digital Agenda (SESIAD) and acts as a point of contact in Spain on cybersecurity. Its activities include research, service delivery and coordination.[73] INCIBE organises workshops together with ENISA which are intended to develop and implement policies and to foster cooperation between the Member States.
INCIBE's expertise and capacity building is in Spanish and limited to stakeholders in Spain. It is however not clear to what extent ENISA can provide additional value to stakeholders in the Member State, specifically through its threat analysis reports, support in the field of critical infrastructures and incident analysis.

The Dutch NCSC conducts very similar activities to ENISA by providing expertise, developing and implementing policies and enhancing capacity building. The National Cyber Security Centre, working under the Ministry of Security and Justice, is the national centre in charge of promoting cybersecurity and ensuring capacity for response in the Netherlands. The NCSC complements ENISA's activities in the area of fostering cooperation between the Member States and other NIS related communities and by conducting cyber exercises with its neighbouring countries. Risks of overlap were identified in the threat analysis reports, provision of good practices, white papers for the Dutch government and trainings which CERTs/CSIRTs attend. Similar to the case of INCIBE, it is not clear whether ENISA's activities in these specific areas are adding to what is done at national level.

---

[71] ENISA (2013): National-level Risk Assessments. Available at: https://www.enisa.europa.eu/publications/nlra-analysis-report/at_download/fullReport.

[72] JRC (2015): Risk assessment methodologies for critical infrastructure protection. Available at:
http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf

[73] https://www.incibe.es/en

The French ANSSI collaborates with ENISA to enhance cooperation and develop policy but activities overlap in the area of providing expertise to stakeholders and some capacity building activities. The National Agency for the Security of Information Systems which works under the General Secretary of Defence and National Security is responsible for promoting cybersecurity and ensuring capacity for response in France. By organising events in collaboration and by supporting ANSSI to foster cybersecurity policy in France, ENISA and ANSSI complement each other. Although ANSSI provides its expertise in the form of reports and recommendations in French, there is a lot of overlap in terms of the topics covered and thus it can be questioned to what extent ENISA's activities are needed in addition.

There is strong coherence between the needs of Member States with fewer resources and capacities, and the services provided by ENISA. The national organisations selected for the positioning exercise are those of Member States with a comparably high budget and capacity in the area of cybersecurity. Many other Member States do not allocate the same resources to cybersecurity and thus rely more on the services provided by ENISA. This is in particular the case in the areas of capacity building, provision of expertise and support in the implementation of policies, as presented in section 3.2.1.4. The evaluation of ENISA's activities in 2015 also found that there is a tendency that Member States with lower NIS capacity or maturity benefit in particular from the exchange of best practice (e.g. on national cybersecurity strategies), while Member States with higher NIS capacity tend to benefit from technical studies, and contribute with best practices. Hence, there is less of a risk of duplication of efforts between ENISA and such Member States where ENISA's spectrum of services area relevant overall.

Stakeholder interviews show that some of the activities are more effective when implemented by ENISA rather than at national level. For other activities the cybersecurity organisations of the Member States assessed in the positioning exercise are better equipped. In general, ENISA's expertise is valued in all Member States as providing an additional, independent source of information. Often the comparison across the EU provides added value. However, some Member States (those with high resources for cybersecurity) were rather critical in the interviews, stating that ENISA's reports did not match the quality and topicality of national-level reports. By contrast, ENISA has developed a strong capacity to bring different stakeholders to the table and ensure cooperation across the EU, adding to the stakeholders that Member States could reach individually when organising events or exercises. With regard to policy development and implementation, Member States' cybersecurity organisations tend to have a more direct link to their government than what ENISA has been able to build. Here national organisations can provide legal and policy input more effectively. Finally, the quality of ENISA's cyber exercises is considered high and allows ENISA to make an important contribution to capacity building, especially in Member States with fewer resources and capacities. However, some of the Member States have organisations which are also strong in providing training and organising smaller scale exercises.

The complementarities and risks of overlap between ENISA and the assessed EU bodies and national organisations are summarised in further detail in Figure 52 below. The activities of ENISA have been structured across the four main tasks: enhancing cooperation, develop and maintain a high level of expertise, enhancing capacity building and developing and implementing policies. Sub-categories of these tasks present more specific activities. A potential overlap of an organisation's activities with those of ENISA is indicated by a visual overlap of the symbol used for an organisation with the blue circle in middle, representing ENISA. The symbols of organisations that do not overlap with the blue circle representing ENISA represent organisations that implement the described activity or service, but where there are sufficient differences (e.g. in the approach, the scope, the target group) in the activities implemented that no potential overlap was identified. The complete assessment on which this figure is based can be found in Appendix 4.

Figure 52: Positioning map

To enhance **cooperation** both between the Member States of the European Union and between related network and information security communities

Cross Member States cooperation building

3

J

ENISA

A

I

C

N

To develop and maintain **a high level of expertise** of European Union actors, taking into account evolutions in network and information security

Good practices and recommendations

I

C

J

J

N

A

A

I

ENISA

I

N

C

N

J

A

C

Regular Threat Analysis reports

Knowledge and methodology enhancements

Incident analysis

Direct support and assistance

C

I

A

3

3

I

C

I

N

C

ENISA

A

3

N

J

A

J

I

Trainings

Standardisation

Good practices, white papers and guidelines

To assist the Member States and the European Union institutions and bodies in **enhancing capacity building** throughout the European Union

Good practices, reports and standardisation for legal and policy areas

C

3

N

ENISA

A

J

I

To assist the Member States and the European Union institutions and bodies in **developing and implementing the policies** necessary to meet the legal and regulatory requirements of network and information security

Legend

C   CERT-EU   **A**   ANSSI   Overlap

3   EC3   **I**   INCIBE

J   DG JRC   **N**   NCSC   Complementarity

3.2.4.4   Procedures to ensure coherence

<div style="border:1px solid #000; background:#cfe2f3">

EQ25: Are the procedures put in place effective to ensure that ENISA's cooperation activities coherent with the policies and activities of its stakeholders?
Only few coordination procedures are in place to ensure coherence. As potential overlaps have been identified there is a need to develop better procedures to avoid overlaps in the future.

</div>

Besides the representation in the Management Board or the PSG, few coordination procedures are in place that aim at ensuring the coherence of ENISA's activities with the policies and activities of its stakeholders. The 2014 and 2015 annual evaluations of ENISA's activities did not identify many formal mechanisms in place to ensure coherence. It can be concluded that based on being represented in the Management Board or the PSG and the feedback process in connection to the work programmes, the Commission, other EU bodies and agencies, and the Member States are able to point to any potential overlaps.

The identified risks of overlap suggest that there is a need to ensure further coordination between ENISA and some of its stakeholders. In particular with CERT-EU there is a need to clarify roles. The Commission foresees to present a cooperation blueprint to handle large-scale cyber incidents on the EU level in the first half of 2017.[74] Based on this, the roles of CERT-EU and ENISA when handling mayor incidents could be clarified. As shown in section 3.2.4.1, there is a need for more trust and willingness to cooperate between the two organisations. In theory, one solution could be to merge ENISA and CERT-EU into one organisation. More generally, there is a need to consolidate the fragmented field of cybersecurity and ensure coordination across the different actors involved at EU level but potentially also beyond.

3.2.4.5   Conclusion on coherence

<div style="border:1px solid #000; background:#e6e6e6">

Conclusion – Coherence

The baseline situation (established based on an evaluation of all EU agencies including ENISA in 2009[75] and an impact assessment of changes to ENISA's mandate in 2010[76]) points to coherence between ENISA and the EU strategies and policies. Unlike over the period 2013-2016, there were no other EU agencies or bodies covering cybersecurity. Therefore no overlaps were identified in the 2009 evaluation.

ENISA's activities are generally coherent with the policies and activities of its stakeholders but there is a need for a more coordinated approach to cybersecurity at EU level. The findings of the evaluation study suggest that the potential for cooperation between ENISA and the European Commission, as well as other EU bodies, is not fully utilised. There is room for more coordination to ensure better coherence and complementarity in order to attain increased NIS in Europe. For example, enhanced coordination between ENISA and the DG JRC would avoid the current (although low) risk of overlap. In addition, the division of responsibilities between ENISA and CERT-EU should be clarified.

ENISA's activities are largely coherent with the work done at national level in the area of cybersecurity. Coherence is particularly strong between the CERTs/CSIRTs and ENISA. Some

</div>

---

[74] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry; COM (2016) 410 final

[75] Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

[76] European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

overlaps between ENISA's activities and those of Member States with strong cybersecurity expertise were identified, but Member States with less capacity and resources in the area of cybersecurity still benefit from these activities.

3.2.5 EU-added value

EU-added value looks for changes which can be assigned to EU intervention, rather than any other factors.[77] To some extent the questions presented below bring together the findings of the previous evaluation criteria. This section responds to prospective questions as listed in the roadmap for the evaluation of ENISA. In addition to the questions from the roadmap, a retrospective sub-section on the added value of ENISA over the years 2013-2016 has been added.

The following questions are responded to in this section:

Table 23: Evaluation questions covered under the EU added value criterion

Main evaluation question	Other evaluation questions
EQ27: What would be the most likely consequences at the EU level of stopping ENISA?	**Retrospective** EQ45: What has been the added value of having an EU cybersecurity agency such as ENISA over the period 2013-2016?[78] **Prospective** EQ28: How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place? EQ35: What would be the most likely consequences at the EU level of stopping ENISA's activities?

3.2.5.1 EU-added value of ENISA

EQ45: What has been the added value of having an EU cybersecurity agency such as ENISA over the period of 2013-2016?
ENISA is providing significant added value to the cybersecurity activities implemented in the Member States. Most importantly, ENISA ensures cooperation in the prevention and mitigation of cybersecurity incidents. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. In addition, the Agency's activities to provide expertise and capacity building represents important added value for Member States with little national resources for cybersecurity.

ENISA fills a gap at EU level. Without ENISA there would be no EU-level mechanism seeking to bring together and bridge the diverse field of cybersecurity. Through its community-building objective in particular, ENISA brings together a variety of stakeholders representing different sectors. As mentioned in section 3.2.2.1, ENISA has made a clear contribution to the overall goal of increasing network and information security in Europe, including by sharing good practices in NIS (as shown in the stakeholder survey carried out by the 2015 evaluation) and through its work on developing networks, the Cyber Europe Exercises and training activities, awareness raising activities and the provision of the Agency's expertise. Stakeholders appreciate ENISA's publications for providing an EU wide overview and perspective on cybersecurity issues which is not available elsewhere.

---

[77] Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

[78] This question has been added by the evaluator based on comments received from the Commission to the Interim Report. It was not presented in the Roadmap for the evaluation of ENISA.

ENISA adds value to the cybersecurity activities implemented by national authorities. Interviews with Member States but also with ENISA's users and advisors show that some of the activities are more effective when implemented by ENISA rather than at national level. In general, ENISA's expertise is valued in all Member States as providing an additional, independent source of information. Often the comparison of threats and chosen responses across the EU provides added value. As the positioning exercise has shown (section 3.2.4.3), ENISA's added value is not the same in all Member States. In Member States with more cybersecurity capacity and resources, national expertise and capacity tends to be better adapted to the national context than what is provided by ENISA. This is also reflected in the responses to the open public consultation where the option "products and services provide unique information (not offered by other bodies or organisations)" was one of the least selected reasons for using ENISA's products or services. However, for Member States with fewer resources, ENISA's capacity building and expertise provides significant added value.

3.2.5.2   Potential to increase added value

> **EQ28: How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place?**
> ENISA could increase its added value by ensuring better coordination with national cybersecurity authorities to ensure that there is no duplication of efforts. Under the current circumstances the Agency could also ensure increased exchange with other EU bodies such as CERT-EU to avoid any overlap. Beyond this, there is very limited scope for any increase in added value as the Agency is restricted by its financial and human resources.

To some extent ENISA could increase its added value by ensuring better coordination with national cybersecurity authorities and other EU bodies. The annual evaluation of ENISA's activities in 2015 suggested that ENISA could increase its added value by avoiding a duplication of efforts in its activities relative to those of Member States with strong cybersecurity capacities and with other EU institutions. This has also been confirmed by the present study (see section 3.2.4). Better coordination of activities with EU level actors in the field of cybersecurity such as CERT-EU and the DG JRC could create new synergies. Similarly, ENISA should continue to ensure that publications are not restating what is already known at national level but provide an added European perspective on a given topic.

The potential to increase the added value of ENISA's contribution to NIS in Europe is limited by the Agency's restricted financial and human resources. Stakeholders' suggestions from interviews across all consulted groups and in general the findings of this study point to a high potential for ENISA to expand and enhance its activities to create more value for its stakeholders. This includes an improved outreach to and cooperation with the private sector, developing and providing more technical expertise, and reaching out to third countries or even globally. However, under the current circumstances, ENISA will not be able to fulfil its potential. The findings of the evaluation show that in the next years ENISA will have to focus its resources on the implementation of the NIS Directive. There is limited capacity and budget available to take on any tasks in addition.

3.2.5.3   Consequences of stopping ENISA's activities

> **EQ35: What would be the most likely consequences at the EU level of stopping ENISA's activities?**
> A discontinuation of ENISA would most likely lead to other organisations taking up part of ENISA's activities. Member States could bilaterally replace some of the coordination efforts and support to CERTs/CSIRTs. The Commission might take on the planned role for ENISA under the NIS Directive.

The consequences of stopping ENISA would be most felt by Member States with fewer resources being invested in the cybersecurity area that would risk falling further behind more advanced Member States. While there might be no immediate severe consequences in stopping ENISA for Member States with greater capacity, it can be considered a lost opportunity over the medium- to long-term. Most stakeholders expect a growing role for ENISA in the coming years to ensure NIS coordination and strengthen resilience in the EU.

There is a need for coordination across the Member States to ensure NIS, therefore without ENISA another way of cooperation will have to be put in place. Most likely ENISA's activities would be dispersed across several organisations. During the interviews ENISA's direct stakeholders suggested that a discontinuation of ENISA would likely lead to more bilateral cooperation between the Member States, but not all the activities of the Agency could be replaced this way. As shown in section 3.2.5.1, ENISA's added value lies in particular in the cooperation across all the Member States and in activities such as the Cyber Europe exercises and the support to the network of CERTs/CSIRTs. In particular for Member States able to invest comparably few resources in the cybersecurity area, ENISA represents significant added value. Interviewees from the EU institutions and bodies suggested an increased role for CERT-EU should ENISA be discontinued, but it was judged that none of the potential organisations that could take on the tasks of ENISA could be considered as a real alternative to having a decentralised agency covering NIS. These services would thus most likely cease to be provided.

According to some of the users and advisors to ENISA, the division of ENISA's activities across different organisations could lead to further fragmentation in the cybersecurity field in Europe as sector specific cybersecurity organisations could be created. Other EU agencies, such as the European Aviation Agency, already have built up some capacities in the area of cybersecurity. Member States investing fewer resources in the cybersecurity area would fall behind in their capacities, ultimately making the entire EU more vulnerable to threats.

Another solution for the implementation of the NIS Directive would need to be identified. A few stakeholders from the EU institutions and bodies suggested that the Commission would have to take on this role, but Member States might be less willing to cooperate directly with the Commission relative to a decentralised agency with a Management Board in which they are represented (and can thus steer the activities to a large extent).

Stopping ENISA would represent a lost opportunity. ENISA is needed over the medium- to long-term for its ability to ensure cooperation across the Member States and most stakeholders see a growing role for ENISA in the future. Many direct stakeholders and users and advisors envisage a role for ENISA in the future as a key player in European cybersecurity and there seems to be no immediate alternative option to ENISA, which is recognised by CERTs/CSIRTs as a trusted partner to ensure cooperation. Many of the interviewed direct stakeholders of ENISA concluded that the most likely consequence of stopping ENISA would be the creation of another agency down the line, potentially with more resources and a stronger mandate than ENISA has now, as an EU agency in the area of cybersecurity is needed.

3.2.5.4   Conclusion on EU added value

Conclusion – EU-added value

The <u>baseline situation</u> (established based on an evaluation of all EU agencies including ENISA in 2009[79] and an impact assessment of changes to ENISA's mandate in 2010[80]) shows the added value of an EU agency covering NIS issues which were found to be more effectively addressed at EU level than by individual Member States. This added value was also identified in the present evaluation study focusing on the 2013-2016 period, as further described below. The evaluation of 2009 found that ENISA was still building up a role which was expected to allow the Agency to delivery "true European value-added" in the future. This was also a conclusion reached as part of the present evaluation based on stakeholder feedback, suggesting that ENISA still has not been able to fully meet its potential.

ENISA's added value lies primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related NIS communities. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. The added value of ENISA differs between Member States, depending on their cybersecurity capacities and resources. The Agency's activities of providing expertise and capacity building represent important added value for Member States with few national resources dedicated to cybersecurity. This is less the case for Member States with more cybersecurity capacities.

Consequently, a discontinuation of ENISA would impact Member States differently. While Member States with strong cybersecurity capacities will be able to replace the services provided by ENISA at least to some extent, this will not be the case for Member States with fewer resources. The latter Member States rely more on ENISA's services in terms of capacity building, access to expertise and support in the implementation of policy and legislation. Cybersecurity crosses borders, so there is a need to build capacity to avoid weaker links that can impact on cybersecurity in the EU as a whole, as well as a need to provide a cross-EU response. It will not be possible to ensure the same degree of community building and cooperation across the Member States without a decentralised EU agency for cybersecurity; the picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA. Therefore, coordination at EU level is needed.

A potential discontinuation of ENISA would be a lost opportunity for all Member States. Most stakeholders were of the opinion that ENISA could take on a more important role in the EU cybersecurity landscape in the future, ensuring a common response capacity. This potential for the Agency to capitalise on future opportunities would be lost should it be discontinued.

---

[79] Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings

[80] European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA), SEC(2010) 1126

3.3 Assessment of ENISA's strength, weaknesses, opportunities and threats

Based on an analysis of the context – namely the evolution, since the last revision of ENISA's mandate in 2013, of the cybersecurity and digital privacy landscape - the evaluation study provides an assessment of the main strengths and weaknesses of ENISA within its current mandate, organisational set-up and resources, in the new cybersecurity and digital privacy landscape. The evaluation study also examines whether a fixed-term mandate is coherent with the new challenges and tasks ENISA will have to take on. In the analysis of the context, the aim of the study is to assess if and how the increase in the frequency, sophistication and potential impact of cyber-threat trigger new needs of ENISA's constituency, and how the changed policy and regulatory landscape, having regard to the recently adopted NIS Directive and the priorities set by the Digital Single Market Strategy impact on ENISA's activities. This allows the identification of opportunities and threats emerging from such a landscape.

This section relates primarily to the prospective aspects of the evaluation study. The table below presents the six evaluation questions which are covered in this section.

Table 24: Evaluation questions covered under the assessment of ENISA's SWOTs

Prospective

EQ36: Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent is ENISA best placed to respond to these needs? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?

EQ37: How does the new policy and regulatory landscape, having regard for the recently adopted Network and Information Security Directive and COM(2016) 410, and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?

EQ38: What are the main strengths and weaknesses of ENISA in taking up new challenges, considering its current mandate and organisational set-up and capacity?

EQ39: If ENISA should take on any new challenges and tasks, would a fixed-term mandate be suitable?

EQ40: Which are the concrete needs and opportunities for further increased practical cooperation with Member States and EU bodies?

EQ41: Which are the concrete needs and opportunities for cooperation and synergies with international bodies working in adjacent fields, like the NATO Cooperative Cyber Defence Centre of Excellence?

EQ42: Could ENISA's mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape or would another EU initiative be more efficient?

This section draws on the summative elements of the assessment of ENISA's performance, governance and organisational structure and of the positioning exercise, as presented in section 3.2 and a review of the evolution, since the last revision of ENISA's mandate in 2013, of the cybersecurity and digital privacy landscape. Based on this, the key strengths, weaknesses, opportunities and threats of ENISA in the current, changed policy and regulatory context are established. In so doing, the section contributes to the more formative, forward-looking dimension of this evaluation and will assist in ascertaining what type of mandate for ENISA would best fit the current, evolving context. A desk-based review of key documents was the main source of information for this part of the study, in addition to in-depth interviews to help identify key opportunities and threats. Moreover, three subcontracted policy, legal and technical cybersecurity experts provided their support on the subject and helped to assess how this has/will impact on ENISA as an organisation and the activities it carries out. Further input was obtained through the open public consultation and the validation workshop.

Subsection 3.3.8 below summarise the preliminary findings and conclusions of this section in the form of an analysis of the different strengths, weaknesses, opportunities and threats faced by

ENISA. The following subsections responds to the prospective evaluation questions of the study. A more comprehensive table, summarising ENISA's SWOTs can be found in Appendix 5.

3.3.1 New needs for ENISA's constituency

EQ36: Does the new scenario with increased frequency, sophistication and potential impact of cyber-threats trigger new needs from ENISA's constituency? To what extent is ENISA best placed to respond to these needs? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?

Although there are differing opinions on which stakeholders make up ENISA's constituency and there are strong divergences in the needs of different stakeholder groups, there is agreement that there are new needs as a result of increased cyber threats. The field most regularly mentioned concerns the rise of the IoT and new demands to increase the safety of connected devices. To respond to these, stakeholders see a need for increased cooperation between different authorities and communities (public and private), increased capacities at Member States level and further research into cybersecurity challenges. ENISA was considered to be able to provide activities that respond to such needs. Many stakeholders agree that a more operational role for ENISA with regard to collecting and sharing information on cyber incidents would be desirable. Although some of the stakeholders from all consulted groups see the NIS Directive as a step towards a more operational role, a majority of consulted stakeholders believe an extended mandate to be necessary to fully address the need for more effective information sharing. In addition, ENISA's current financial and human resources are perceived to be insufficient to address these needs.

ENISA has a constituency with diverse needs. Interviewees' opinions differ on which stakeholder groups make up ENISA's constituency. Some of ENISA's stakeholders across all groups even criticise ENISA for the lack of a clearly defined constituency. According to certain interviewees (including Member States), this is sometimes reflected in ENISA's deliverables in terms of inappropriate writing style and dissemination channels to reach the intended target audience. ENISA's direct stakeholders noted that ENISA's role concerning Member States' needs requires clarification because of the strong differences between more experienced and resourced Member States and Member States which are more limited in their capacity and resources. Also the extent to which ENISA should prioritise the support to EU institutions requires clarification. Arguably, Member States are ENISA's primary stakeholders. As shown in the section on relevance (3.2.1), the demands and priorities vary from one Member State to another. There is a tendency for Member States with more resources and capacity in cybersecurity to be less dependent on ENISA and to see the Agency's role in responding to cybersecurity needs as more limited than other Member States. Meanwhile, a number of stakeholders from industry see a need for more action of direct benefit to industry.

There is a wide spread perception that the increased frequency, sophistication and potential impact of cyber-threats triggers new, and reinforces current, needs from ENISA's constituency. The majority of the interviewed stakeholders from all groups view that there are increased risks, in particular in relation to the rise of the IoT and new demands to increase the safety of connected devices. In this regard, rapidly evolving cyber threats create a need for more rapid responses. In line with this, "cooperation across Member States in matters related to cybersecurity" and "the capacity to prevent, detect and resolve large scale cyber-attacks" were identified by the largest number of respondents to the open public consultation as a main gap or need in the cybersecurity field in the EU over the next ten years. A majority of the respondents in each of the three categories of respondents (i.e. national authorities, private enterprise or business association, and other) were of the opinion that these were needs or gaps, as Figure 53 illustrates. Respondents that commented in their open responses on the need for increased cooperation across Member States suggested that cooperation was necessary not only to bridge the security gaps that arise from a lack of cross-country cooperation, but also to build trust

and confidence within the EU in matters of cybersecurity. Some respondents (including Member States) pointed to additional benefits of such cooperation, including increased market integration through the provision of internet services, support to the increase in cybersecurity capacity of less advanced Member States, and innovation for responses to current and future threats. Additionally, three respondents referred to an additional need, namely the need for "effective international cooperation" (i.e. EU and third countries such as the US, Japan, Korea and India). Comments on the need to increase capacity to prevent, detect and resolve attacks pointed to the fact that the EU should step up the detection and real-time response to cyberattacks in information, communication technology (ICT), critical infrastructures, SMEs, government and public agencies. Others felt that while detecting and responding to cyberattacks is important, the priority should be placed on developing a prevention-focused approach that allows protection from loss of intellectual property and personal data as well as loss of trust. The views of the different open public consultation respondent groups in relation to each of the options were relatively balanced, with the notable exception - among the most referred to gaps or needs - of "cooperation and information sharing between different stakeholders, including public-private cooperation" where only two national authority respondents (out of a total of 38 respondents) identified it as a need or gap.

Figure 53: Most urgent needs or gaps in the cybersecurity field in the EU in the next ten years (multiple choice question)
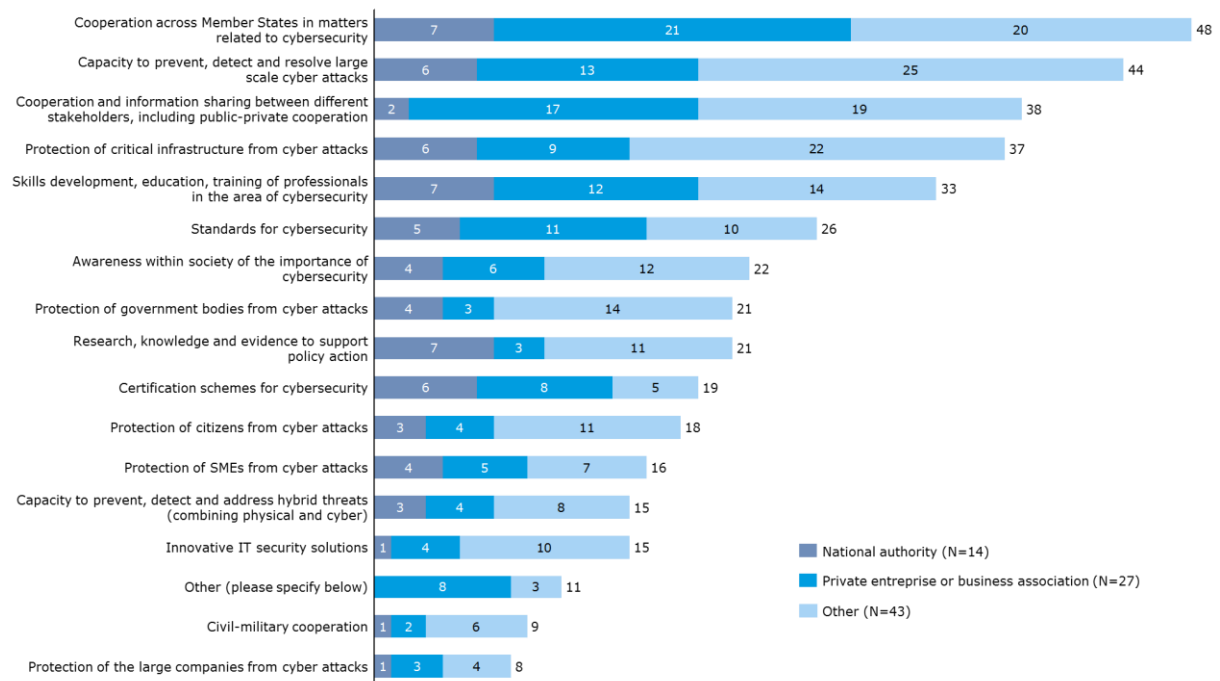
Source: Open public consultation

Instruments and mechanisms at EU level were not judged fully adequate to promote and ensure cybersecurity within such a context. Taking into consideration the above mentioned needs, only 6% of the open public consultation respondents judged the current instruments and mechanisms at European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be fully adequate to promote and ensure cybersecurity. A great majority of the respondents (including Member States) regarded them as partially adequate or only marginally adequate (52% and 31% respectively) and 5% found them not at all adequate. As shown in Figure 54below, national authority respondents appear to be more positive about the adequacy of these instruments and mechanisms in comparison with representatives from private enterprises or business associations and other respondents.

Figure 54: Adequacy of current instruments & mechanisms at European level to promote and ensure cybersecurity

| | National authority (n=14) | Private enterprise and business association (n=27) | Other (n=43) |
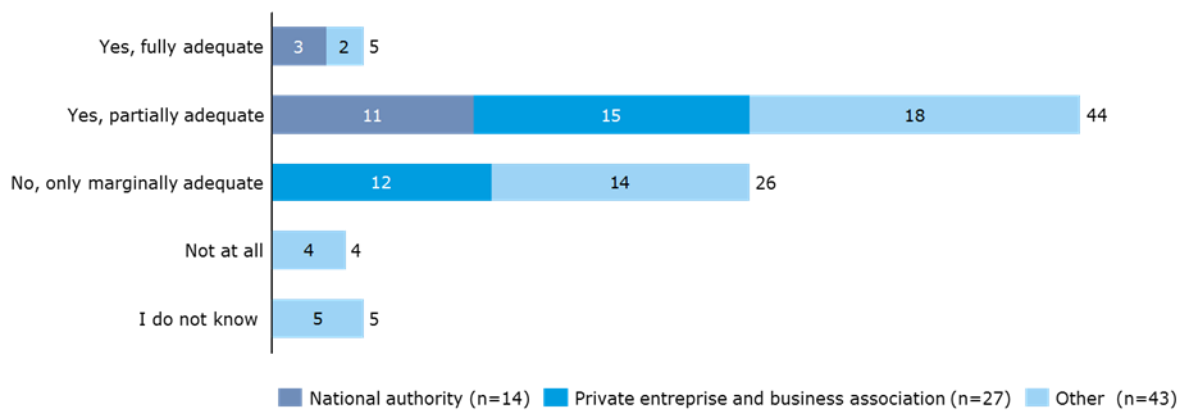
Source: Open public consultation

The open public consultation respondents were asked to elaborate on their answers and 51 contributions were received, providing further assessments and recommendations for improvement. Some examples of the inputs from respondents who assessed the current instruments and mechanisms as "partially adequate" are summarised here. In their comments respondents positively assessed the progress the EU has made in the set-up of its *regulatory and institutional framework* for cybersecurity. However, respondents also felt that the majority of the instruments have yet to be implemented, enter into force or still need to be developed. Three respondents stated that the framework is too often open to interpretation, which "leaves the possibility of non-harmonised implementations" that are contrary to its aim. Considering the fast-paced development of technology and cybersecurity needs today, respondents recommended that current policy instruments continue to evolve, change and adapt: "it is therefore important that the European agencies and bodies assess and evaluate the cybersecurity landscape to ensure the needs of the governments, industry and citizens are being met". It was also suggested that cooperation mechanisms created by the *NIS Directive* should be evaluated after two years. Other respondents commented that the development of *standardisation and certification* regarding information security at EU level should be improved and accelerated. As a final example, on *IT solutions* respondents felt Internet-of-Things-risks ought to be addressed more strongly and EU-made cybersecurity solutions developed by the private industry (SMEs) should be supported.

Enhanced cooperation between Member States and with the private sector is considered to be the primary solution to the new and enhanced needs of ENISA's stakeholders. Based on the identified needs or gaps, open public consultation respondents were asked to consider what the priorities for EU action should be from now on and select up to three responses out of a list of 15. As revealed in Figure 55 below "stronger EU cooperation mechanisms between Member States, including at operational level" was clearly considered to be the most important action, followed by "stronger public-private cooperation in cybersecurity" and "improving research to address cybersecurity challenges". When analysing the number of responses from the three different groups of respondents, considering also the size of each group, it can be noted that the action "improving education and curricular development in cybersecurity" received relatively higher support from "other" respondents. In contrast, the action "improving capacity in Member States through training and capacity building" was comparatively more supported by national authorities. It should also be mentioned that three of the actions were not selected as a priority by any national authority representative, namely: "stronger cooperation between different authorities and communities (e.g. between CERTs/CSIRTs and law enforcement authorities; Information Sharing and Analysis Centres and CERTs/CSIRTs)", "stronger cooperation between civil and military cybersecurity authorities and organisations", and "improved monitoring of threats and incidents across Member States".

Figure 55: Top priorities for EU action from now on in the area of cybersecurity
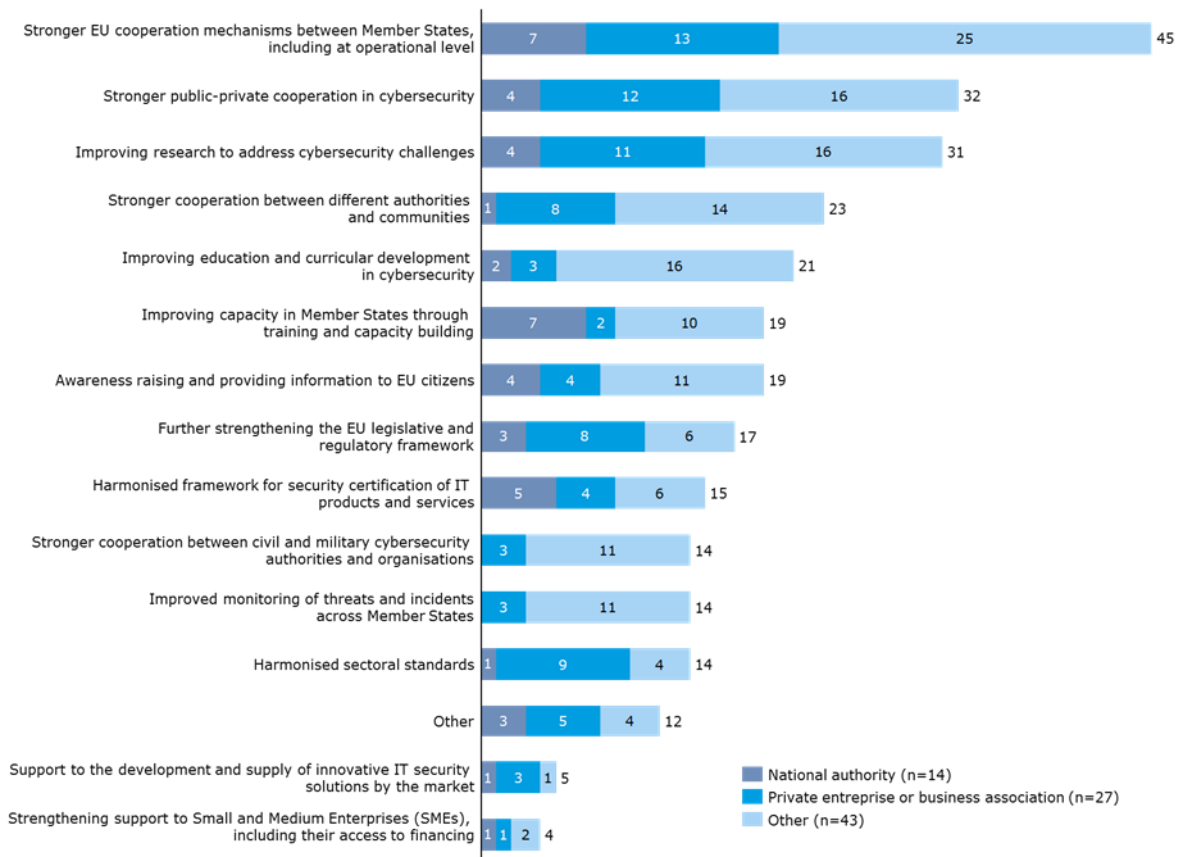
Source: Open public consultation

Among the twelve open responses who selected the option "other" (see Figure 55 above), fourteen additional "top priorities for EU action" were identified. Among these, six of the priorities mentioned were also related to *cooperation*. Besides pushing for "stronger public-private cooperation" respondents pointed to "establishing stronger international / trans-Atlantic cooperation and collaboration" including regulatory convergence, as well as "developing policy and operational support for cooperation and information sharing between different stakeholders and Member States". Five priorities mentioned concerned *support and guidance*, e.g. "Support uptake of new privacy techniques", "Improved monitoring of threats", "Provision of implementation, application and enforcement tools" and an "EU-reviewed open source, for public administration i.e. communes". Finally, three matters related to *cybersecurity regulation* and the respondents asked for "more flexibility in regulation to allow adapting to nature of organisations, services and markets" and believed that ENISA's role in relation to this should be that of "sign-posting relevant and robust standards that function at global level" given its "important role in harmonisation across the EU".

ENISA is expected and considered capable of taking on a role in responding to stakeholder needs in the future. Following on from the assessment of needs, gaps and top priorities for action, the open public consultation respondents were asked about ENISA's future role. As illustrated in Figure 56 below, 98% of respondents (82) thought that there is a role for an EU-level body in improving cybersecurity across the EU.

Figure 56: Is there a role for an EU-level body in improving cybersecurity across the EU?

Legend:
- National authority (n=14)
- Private enterprise & business association (n=27)
- Other (n=43)
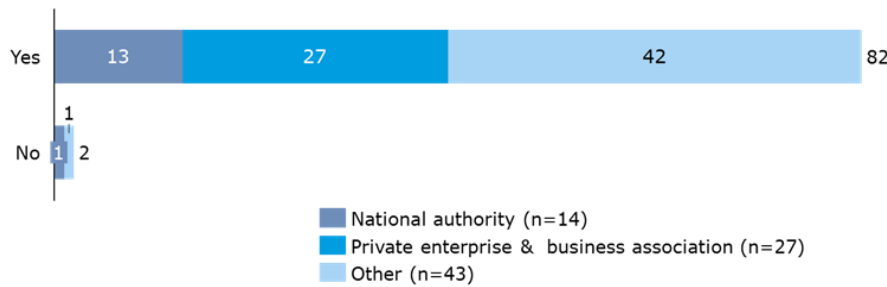
Source: Open public consultation

Furthermore, almost all of the respondents (81 of 82) who saw a role for an EU-level body in improving cybersecurity considered that ENISA could fulfil a role in bridging the different gaps in the future. The Agency, if sufficiently mandated and resourced, was perceived as *most able* to contribute to the following five areas (percentages and numbers reflect respondents that considered ENISA to be able to a *high extent or to some extent* to fulfil a specific role; see Figure 57 below for further details):

- Stronger cooperation between different authorities and communities, 89% (71);
- Stronger EU mechanisms between MS, including at operational level, 87% (69);
- Improve capacity in Member States through training and capacity building, 82% (65);
- Stronger public-private cooperation in cybersecurity, 82% (65); and
- Improving research to address cybersecurity challenges, 82% (65).

In summary, open public consultation respondents consider ENISA to be the right body to respond to the needs they identified as most pressing. In-depth analysis of the answers indicates clear differences in opinion per type of respondent group in some areas. In this sense "stronger cooperation between different authorities and communities" was less supported as a role for ENISA by national authorities (69% selected to a high extent or to some extent) compared to private enterprise & business association (92%) and other respondents (93%). In similar manner "stronger public-private cooperation in cybersecurity" received higher support from private enterprise & business association (96% selected to a high extent or to some extent) compared to national authorities (69%) and other respondents (76%).

Figure 57: Gaps and needs for which ENISA is perceived to be most able to fulfil a role

Legend: High extent | Some extent | Limited extent | Not at all | Don't know
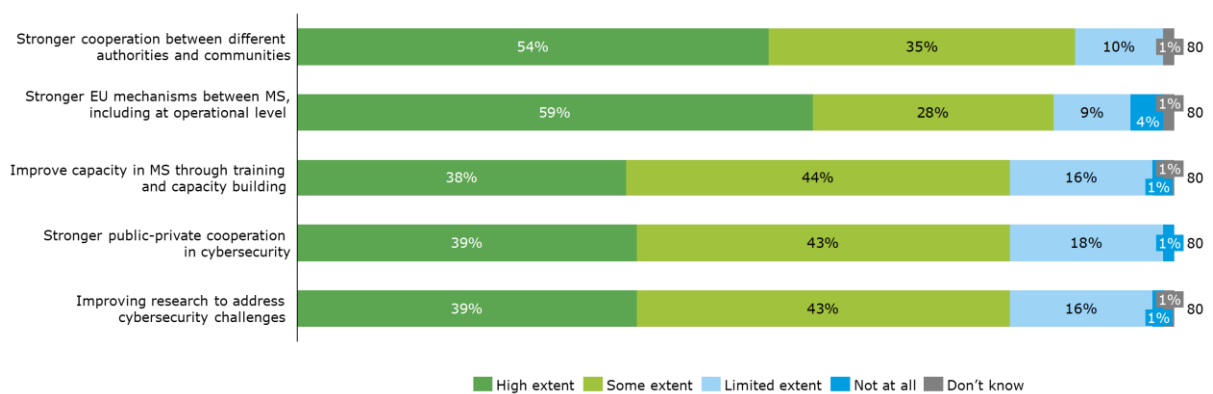
Source: Open public consultation

The gaps and needs for which ENISA is perceived to be least able to fulfil a role correspond with the needs selected by fewer open public consultation respondents as being urgent, as presented in Figure 58.

Figure 58: Gaps and needs for which ENISA is perceived to be least able to fulfil a role

	High extent	Some extent	Limited extent	Not at all	Don't know
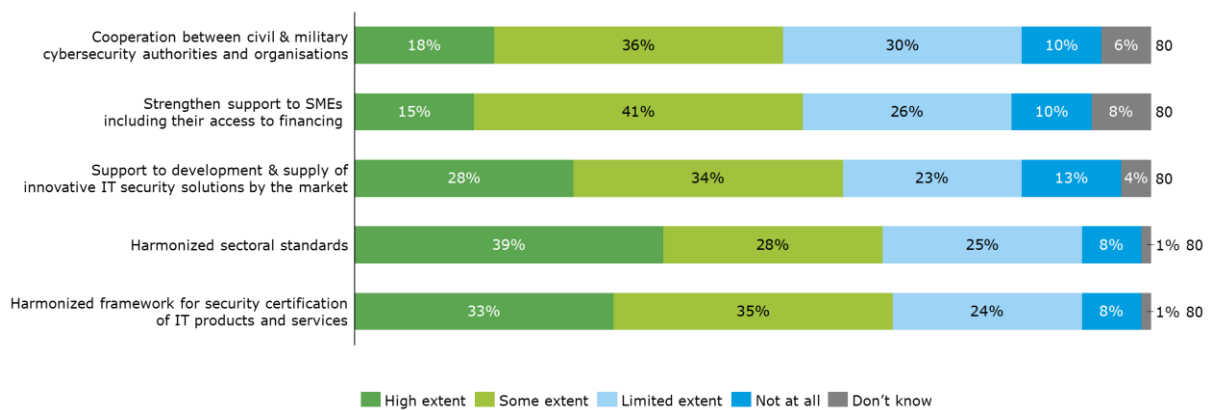
Source: Open public consultation

A variety of suggestions of tasks and activities that ENISA could add to its portfolio to further increase network and information security in the future were made by stakeholders. Interviewees and respondents to the open public consultation made the following suggestions for ENISA to expand its tasks and contribute even more to NIS in Europe:

- Increase the Agency's visibility and involve a broader group of stakeholders in the activities, including capacity building and awareness raising in the private sector and civil society
- Develop more internal expertise rather than providing support based on data collected from other experts; taking on research on cybersecurity in cooperation with research centres
- Cover the areas of standardisation and certification
- Build more trust between the Member States to increase willingness to exchange information on threats and incidents. This could be based on further capacity building in less experienced Member States.
- Work closer together (possibly even merge) with other EU institutions such as Europol's EC3 and CERT-EU
- Enhanced cooperation with third countries, in particular with CERT-equivalents to obtain timely information on cybersecurity threats and incidents to diffuse across the Member States.

Interviewed Member State authorities suggested that ENISA's current tasks which will increase in relevance over the coming years include the Cyber Europe Exercises, training of Member States and fostering cooperation between the cybersecurity communities.

Industry stakeholders would like ENISA to respond more to their needs in the future. The interviewed industry representatives saw an important role for ENISA in acting as a link between the public and private sector. This was confirmed in the open public consultation. The Agency could support industry in the future by ensuring harmonisation of baseline requirements for cybersecurity across the EU. Also a more operational role for ENISA to collect data on threats across the EU and make this data available to the industry would be welcomed by these stakeholders. Some areas that ENISA should be focussing on more as priority areas than is currently the case, according to industry stakeholders in particular, included the Internet of Things, certification and standardisation, the move to big data and machine intelligence, and becoming more active in the educational field, e.g. by supporting the creation of Massive Open Online Courses (MOOC) in the field of cybersecurity.

Many of ENISA's stakeholders - beyond its group of direct stakeholders - see a need to extend ENISA's mandate to embrace more operational roles. In particular, industry stakeholders regularly advocate ENISA taking on a more operational role to collect data on threats and cybersecurity incidents across the EU and share this information with industry. A few comments from the open public consultation respondents relating to this matter largely confirm

that the group of private enterprises & business associations is more positive about ENISA taking on a more operational role, while national authorities are less supportive of such a development. Findings from the workshop revealed equally that the majority of stakeholders see a need for a clearer definition of the term "operational", as it is currently used by many as a synonym for information sharing while others understand it to mean actual response to incidents. During the workshop some of ENISA's direct stakeholders suggested that there could be some interest in enhanced cooperation on threat intelligence/situational awareness led by ENISA. While some interviewees indicate that the NIS Directive already goes in this direction, the majority thought that a review of the current mandate would be necessary for ENISA to be more actively involved in information sharing on cybersecurity incidents.

A concern voiced among all consulted stakeholder groups was whether ENISA would be able to take on the new needs of its constituency given its currently limited resources. In light of the multiple obligations of ENISA today and the identified difficulties to fully respond to stakeholder needs over the period 2013-2016, there is a certain degree of doubt on the extent to which ENISA will be able to respond to the new needs of stakeholders with its current financial and human resources. This is in particular the case considering the additional tasks under the NIS Directive (presented in the following section) which will require an important share of ENISA's staff in the coming years. A majority of the interviewees think that the scope of the Agency's work will further grow in the future.

3.3.2   The impact of new policy and regulatory landscape on ENISA's activities

> **EQ37: How does the new policy and regulatory landscape, having regard for the recently adopted Network and Information Security Directive and COM(2016) 410, and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?**
> There is agreement among all of ENISA's consulted stakeholders that ENISA as the main European entity mandated will be affected by the NIS Directive in multiple ways. While the NIS Directive is seen as an opportunity for ENISA to increase its influence in the current fragmented EU cybersecurity policy landscape, many of ENISA's direct stakeholders, users and advisors see challenges for ENISA in terms of financial and human resource constraints and the risk of overlap with other agencies, above all CERT-EU.

The NIS Directive will have a notable impact on ENISA's activities. There is consensus among all stakeholder groups that the NIS Directive will have a significant impact on ENISA's activities since ENISA is mandated to be the main European entity supporting the transposition of the Directive in the Member States. Several direct stakeholders refer to a large initial impact on ENISA's organisation and activities, but interviewees' opinions differ as to whether this is a temporary effect or whether it will be more long-lasting. A few experts even refer to the NIS Directive as being a "main disruption" and "game changer" in EU cybersecurity policy foreseeing long-lasting changes.

The view of the majority of stakeholders is that the NIS Directive is an opportunity for ENISA to increase its influence. The general perception is that the NIS Directive strengthens ENISA's influence within EU cybersecurity policy by giving the Agency a more operational role in supporting its implementation by the Member States. However, some observers voiced concern about whether the Agency is taking full advantage of the opportunity it is being provided with or whether it is acting too prudently. On the other hand, certain direct stakeholders of the Agency pointed out that ENISA is not equipped with a right to initiate action, but limited to proposing things to the Commission.

The implementation of the NIS Directive currently takes up a large part of ENISA's resources which poses a challenge for the Agency. As presented in section 3.2.1.5, the NIS

Directive is perceived as not only impacting on ENISA's type of activities but also on increasing the overall volume of its responsibilities and work load. According to some of ENISA's direct stakeholders, the Work Programme is currently dominated by the NIS Directive with around 20 staff members having been designated to be work on the NIS Directive. Several interviewees (including Member States) think that without a corresponding increase in financial and human resources, or a reduction of ENISA's activities in other topics, the additional tasks imposed by the NIS Directive are very challenging (by a few even considered impossible) for the Agency to perform. As a result, a number of direct stakeholders of ENISA point out that a potential threat for ENISA lies in capacity constraints to fulfil other tasks to the high standard. However, a few of those stakeholders (including Member States) are more optimistic seeing these challenges to be only temporary until the NIS Directive's transposition in Member States.

Despite the opportunities provided, there are risks of overlap with CERT-EU. The positioning exercise (section 3.2.4.3) detected a risk for overlap between ENISA and CERT-EU; this might increase in the future. Interviewed stakeholders described ENISA's role in supporting the national CERTs/CSIRTs as foreseen under the NIS Directive as more operational and several stakeholders across all consulted groups perceived this new role to create (or increase the risk for) overlaps and conflicts of interest with CERT-EU. Examples referred to include the fact that CERT-EU already implements activities that could fall within the scope of ENISA's mandate by working with stakeholders that are among ENISA's constituency (and go beyond CERT-EU's main constituency of the EU institutions) or by getting in touch with commercial organisations through the use of CERTs/CSIRTs. One of ENISA's direct stakeholders argues that the best option would have been to create CERT-EU as a part of ENISA from the start, but indicates that resistance from some of the Member States prevented this from occurring.

ENISA's new role as the main body mandated to assist national CERTs/CSIRTs puts higher requirements on ENISA to be better connected geographically. Some interviewed stakeholders (including Member States) stakeholders consider that the new obligations under the NIS Directive, e.g. working with the national CERTs/CSIRTs, require increased co-operation with other EU-bodies, in particular with CERT-EU. Following this argumentation, there is a need for ENISA to be more agile and connected to the cybersecurity policy environment.

3.3.3 Main strengths and weaknesses of ENISA

EQ38: What are the main strengths and weaknesses of ENISA in taking up new challenges, considering its current mandate and organisational set-up and capacity?
The assessment of the main strengths and weaknesses of ENISA in taking up new challenges indicates that, in the current set-up, ENISA's weaknesses outweigh its strengths. With regard to the Agency's strengths, the perception of ENISA as a neutral facilitator, mediating the divergent policy priorities of Member States, has helped it gain trust at European level. Its role in fostering collaboration, community building, as well as supporting Member States in their cybersecurity capacities, also deserve a mention. However, ENISA is faced with many obstacles. Given its lack of expertise, weak communication and marketing, and limited self-assertion within the EU cybersecurity landscape, ENISA lacks overall visibility. ENISA also lacks a long-term vision, often being constrained by its fixed mandate and annual work programme. Finally, ENISA lacks resources, both financial and human, in terms of the Agency's limited size and the staff's composition which is being aggravated by the NIS Directive. In addition, ENISA's split location in Athens and Heraklion causes difficulties for the Agency for attracting and retaining qualified staff members.

ENISA's strengths in taking up new challenges

ENISA is perceived as a "trusted" actor[81] **within the EU's cybersecurity policy landscape, free from commercial interests or political bias.** As presented in section 3.2.2.2, one of the main strengths of the Agency is its reputation as an independent and neutral facilitator[82] that is capable of navigating a highly fragmented policy domain, while also being faced with the different priorities of Member States.[83]

Furthermore, collaboration and community building belong to the Agency's core strengths. As presented in section 3.2.1.4, ENISA has proven its capability to maintain a viable network with a range of different stakeholders including national governments, industry, the EU institutions and other EU and international bodies. ENISA acts as a node to gather and exchange information and best practices among Member State, EU and international players. ENISA is also involved in fostering cooperation with the private sector and encourages the setup of PPPs as a way to increase the operational capabilities in the sector.[84]

ENISA maintains good and recognised working relationships with its direct stakeholders. The survey of ENISA staff and direct stakeholders further shows that the Agency's relationship with its stakeholders and its efforts for cooperation were particularly well considered. A vast majority of 93% of respondents (including Member States) thought that ENISA had built strong and trustful relationships with its stakeholders when executing its mandate. Furthermore, 93% of the survey respondents agreed to some or to a high extent that ENISA was open to cooperating with a variety of stakeholders. Meanwhile ENISA's systems and procedures in place for stakeholder consultation and management were considered to be well-working by 84% of respondents.

ENISA is very active in capacity building assistance. This includes organising trainings, cybersecurity exercises, development of manuals, studies trying to reach a broad sector including Member States, private actors, EU institutions and agencies. The aim of this capacity building activity is to develop the capabilities of the agents, providing them with the necessary tools to prevent, detect and handle incidents.[85]

The organisational solutions and procedures of ENISA were ranked positively by ENISA's stakeholders. As presented in section 3.2.2.8, 80% of survey respondents[86] regard the current solutions and procedures as adequate. Moreover, the current governance structure, with a Management Board, an Executive Board and the PSG, was assessed as conducive both to the effective functioning of the Agency (i.e. in terms of meeting its objectives) and to the efficient functioning of the Agency (i.e. in terms of value for money), by 85% of the respondents in both cases. Finally, 73% and 74% of respondents respectively saw ENISA's management practices as conducive to creating an effective organisation and an efficient organisation to some or to a high extent.[87]

---

[81] See section 3.2.2.8 for further information.

[82] Finding obtained from interviews with ENISA's direct stakeholders.

[83] See section 3.2.1.5 for further information on diverging priorities of Member States.

[84] See, for example: Carrapico, H., Barrinha, A. (forthcoming). The EU as a coherent (cyber)security actor; Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017; ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0; ENISA (2016) Evaluation Roadmap 25/07/2016.

[85] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0;
ENISA (2016) Evaluation Roadmap 25/07/2016; ENISA (2015). Threat Landscape and Good Practice Guide for Software Defines Networks/ 5G: ISBN: 978-92-9204-161-8, DOI: 10.2824/67261.

[86] Source: The survey on ENISA's governance, organisational set-up and working practices

[87] See section 3.2.2.8 for further information.

As the European cybersecurity agency ENISA has significant horizontal expertise to assess how every EU Member State is performing in cybersecurity. ENISA is equipped with a broad mandate, allowing it to take on a wide variety of different tasks ranging from capacity support of Member States to the development of cybersecurity reports/expertise. Thanks to Article 14, ENISA is able to react to ad-hoc requests from the EU institutions and Member States in the field of policy development and policy implementation. This mechanism is used by some of the Member States (see section 3.2.2.6).

ENISA's weaknesses in taking up new challenges

A recurring finding from interviews with ENISA's users and advisors is the Agency's limited visibility. Several root causes are identified to play a part in this: ENISA is seen to lack, in particular technical, expertise and it has relatively weak communication and marketing, giving it marginal presence in the press and media. Indeed, other European agencies, e.g. Europol, FRA or the European Food Safety Authority, have managed to be more present in the media and the public. Potentially as a result of its limited visibility, ENISA has not managed to carve out its own space in the EU's cybersecurity landscape. A few interviewed industry stakeholders expressed their support for the Agency more strongly engaging in commenting on headline events, such as major cyber-attacks on governments or companies in Europe, in order to increase the visibility of ENISA. It should be noted though, particularly in the case of governmental attacks, that ENISA would probably need the prior approval of the impacted Member State to be able to do so.

ENISA lacks a more strategic, long-term vision. Unlike other EU agencies, ENISA has a fixed mandate which in the eyes of a few users and advisors is counterproductive to developing a more strategic, long-term vision. Furthermore, Member States' dominance in the Management Board often leads to an annual work programme characterised by the individual priorities of Member States rather than a more strategic approach to cybersecurity. Finally, a few of ENISA's users and advisors perceive ENISA as being too tied to fulfilling its work programme, contributing to the lack of a strategic approach.

An important weakness concerning ENISA's organisational set-up and capacity relates to its limited size and financial resources. The surveyed group of all stakeholders[88] provided the least positive assessment of the size of the Agency among all elements in the Agency's organisational set-up, with 51% of them perceiving it as being only appropriate to a limited extent or not at all appropriate to the work entrusted to ENISA and to its workload. ENISA's surveyed direct stakeholders were by far the most pessimistic about its size. The open public consultation results overall confirmed this finding as 58% of respondents considered the size of the Agency to be partially or completely inadequate, with no major differences among different respondent groups having been identified. Negative assessments concerning the size of ENISA by interviewed experts – direct stakeholders as well as users and advisors – were often accompanied by comments on a need for more financial resources. The majority of interviewees (including Member States) saw a need to increase ENISA's staff and resources with a few referring to a drastic increase, e.g. doubling the currently available resources. A number of interviewees also pointed out that the NIS Directive placed an additional burden on the Agency without reducing its other tasks or increasing its resources.

Another tangible weakness with regard to ENISA's organisational set-up relates to ENISA's split office location in Heraklion and Athens. While the survey findings only point to ENISA's location being a moderate weakness, the majority of interviewees (including Member States) regard the Agency's location as a major weakness. Accordingly, ENISA's location was reviewed by 67% of surveyed respondents[89] as enabling, to some or to a high extent, ENISA to effectively conduct its work (i.e. in terms of meeting its objectives) and by 59% to conduct its

---

[88] Source: The survey of ENISA staff and direct stakeholders
[89] Source: The survey on ENISA's governance, organisational set-up and working practices

work <u>efficiently</u> (i.e. in terms of value for money). The location was reviewed as not enabling such <u>effectiveness</u> and <u>efficiency</u>, or only to a limited extent, by 28% and 35% of surveyed respondents respectively. From the surveyed respondents, ENISA's direct stakeholders were most critical of ENISA's office location.[90] Meanwhile, all groups of consulted stakeholders were very critical of the office location's impact on the Agency.

One of the arguments supported by a certain number of respondents is that ENISA's effectiveness is impacted by being too far from Brussels, hence complicating ad hoc exchanges with the EU institutions. Various respondents were also critical of the fact that the Agency is divided in two, which decreases its efficiency by creating additional costs and requiring additional efforts to ensure internal communication. Meanwhile, all of ENISA's consulted stakeholder groups admit that the establishment of an office in Athens improved the situation, in particular for the travel of ENISA's stakeholders. Respondents also indicated that ENISA's location is not fit for recruiting and retaining qualified staff due to the lack of facilities for international employees and their families, as well as the low pay and economic uncertainties faced by Greece.

The staff composition of ENISA presents a more moderate weakness. Approximately 65% of surveyed respondents[91] viewed the Agency's staff composition as adequate for its work to some or to a high extent, while 30% viewed it as only adequate to a small extent or not at all. ENISA staff was particularly critical with more than one third of the respondents seeing the staff composition to be adequate only to a limited extent or not at all. Some recurring, highlighted weaknesses concern the need to develop more internal expertise by hiring *more senior staff*, and the need for *more technical staff* to improve the balance between administrative staff and operational staff. Some of ENISA's direct stakeholders also reported that the Agency's recruitment difficulties had led to an over-representation of Greek nationals in ENISA with often low incentives for job rotation.

Along with the staff composition, the recruitment and training procedures can be considered a moderate weakness. Among the surveyed respondents, 33%[92] found the recruitment and training procedures of ENISA not to be appropriate or to be only appropriate to a limited extent to manage ENISA's workload. Additional comments revealed that the recruitment *process is considered too slow* and therefore not well adapted to the cybersecurity domain which is fast paced. The *lack of training* that the staff experienced over the five years prior to writing was linked to the *absence of a dedicated HR department within* the Agency.

3.3.4   Format of ENISA's mandate

> **EQ39: If ENISA should take on any new challenges and tasks, would a fixed-term mandate be suitable?**
> Clear advantages for ENISA having a permanent mandate were identified. This would allow it to develop a more long-term strategy and increase its effectiveness. It could also alleviate current recruitment difficulties. A permanent mandate should not exclude the need for regular evaluations and revisions of ENISA's mandate.

The findings from the interviews show that views diverge on whether a fixed-term mandate would be suitable to help ENISA take on new challenges and tasks. ENISA's Regulation foresees an end date by which the Agency' mandate expires. Among the EU agencies, ENISA is the only one with such a mandate since the European Agency for Reconstruction was

---

[90] See section 3.2.3.1 for further information.

[91] Source: The survey on ENISA's governance, organisational set-up and working practices

[92] Ibid.

disbanded in 2008.[93] Many direct stakeholders see clear benefits in ENISA having a permanent mandate. The reasons for supporting a permanent mandate are linked to allowing ENISA to plan over the longer term and support the development of a greater vision. Aside from generating greater independence, these stakeholders also claimed that a permanent mandate would lead to more effectiveness. However, others were more in favour of a fixed-term mandate, thinking that this would provide for greater levels of flexibility to adapt the Agency's mandate to the rapidly evolving cybersecurity landscape. Another recurring view in support of a fixed-term mandate was that ENISA's performance could be more easily evaluated or re-evaluated in the case of changing needs. Yet, supporters of a fixed-term mandate also admitted that it can cause negative side effects, such as the Agency's recruitment problems and political uncertainty. In the discussion at the workshop, a clear preference was shown for a permanent duration of the Agency with a mandate that is evaluated and reviewed every few years, as is the case for other EU agencies.

3.3.5 Concrete needs and opportunities for practical cooperation with Member States and EU bodies

> **EQ40: Which are the concrete needs and opportunities for further increased practical cooperation with Member States and EU bodies?**
> With regard to practical cooperation with Member States, stakeholders agree that this needs to be further increased, in particular with the CERTs/CSIRTs. Aside from providing direct support and helping CERTs/CSIRTs to respond to the requirements under the NIS Directive and to further build their capacity, additional training and increased interaction between ENISA and the CERT/CSIRT community were found to be important.
>
> With regard to cooperation between ENISA and other EU bodies, only few consulted stakeholders suggested that there was a need to increase the interaction. However, the fragmentation of cybersecurity across different DGs of the European Commission and agencies, shows that there is in fact a need to enhance cooperation and coordination.

Cooperation with Member States was seen as one of the top priorities to respond to stakeholder needs, while less emphasis was put on cooperation with EU bodies. The findings of the open public consultation showed that stakeholders expect ENISA to further foster increased Member State cooperation to respond to new and reinforced cybersecurity challenges, as presented in section 3.3.1. Fewer open public consultation respondents and interviewed direct stakeholders of ENISA considered cooperation between ENISA and EU bodies as a priority. Nevertheless, interviews with representatives from the Commission, other EU agencies and ENISA's staff, as well as the assessment of ENISA's coherence (see section 3.2.4), show that there is a need to enhance cooperation and coordination across EU bodies to create synergies and develop an EU approach to cybersecurity.

ENISA's new role under the NIS Directive will allow the Agency to better address the needs of CERTs/CSIRTs. An overwhelming majority (85%) of the respondents to the CERT/CSIRT survey were of the opinion that the new role foreseen for ENISA in relation to CERTs/CSIRTs as part of the NIS Directive will enable ENISA to better cover CERTs/CSIRTs' needs. With respect to the activities to be carried out by ENISA, facilitating cooperation was seen as key by a large number of respondents. Fields where further assistance of ENISA would be useful included better understanding the needs of CERTs/CSIRTs and providing direct support and helping CERTs/CSIRTs implement the NIS Directive and build capacity. In terms of what ENISA could do to better cover CERTs/CSIRTs' needs, more trainings and increased interaction of ENISA with CERTs/CSIRTs were seen as particularly important by respondents. The call for more training opportunities is largely confirmed by the different stakeholders. A few interviewed users and

---

[93] European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No4 – Ending of agencies. Available at: http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_4_sent_to_ep_cons_2010-12-15_en.pdf

advisors particularly point towards the opportunity for ENISA to train the trainers, i.e. to develop harmonised European training packages on different levels – from the citizens to the professionals and decision-makers – to be used by the Member States.

3.3.6   Concrete needs and opportunities for practical cooperation with international bodies

EQ41: Which are the concrete needs and opportunities for cooperation and synergies with international bodies working in adjacent fields, like the NATO Cooperative Cyber Defence Centre of Excellence?
All groups of consulted stakeholders were generally in favour of increased cooperation with international bodies and several examples of such bodies were presented as opportunities for future cooperation. These concern, for example, the United Nations' International Telecommunication Unit (UN/ITU), the Forum of Incident Response and Security Teams (FIRST), the US National Institute of Standards and Technology (NIST) and third country governments. However, with respect to the North Atlantic Treaty Organisation (NATO), stakeholders' views on the possibilities for efficient collaboration differed significantly.

There is a strong consensus among ENISA's direct stakeholders, advisors and users that increased international collaboration is important, however, opinions differ on whether NATO is the most appropriate partner. A majority of the interviewed stakeholders were supportive of increased cooperation with international bodies working in adjacent fields. The open public consultation confirmed this, showing that several respondents suggested that there is a need for more international cooperation but suggested approaches focussed on direct cooperation with third countries. Some direct stakeholders indicated in the interviews that there are both strong needs and good opportunities for collaboration with NATO and that there is a movement in the direction to combine civil and military aspects of cybersecurity. However, other direct stakeholders as well as advisors and users were either sceptical of the benefits of collaboration or indicated barriers to it, mainly in the form of reluctance and lack of trust from some Member States (e.g. not all Member States are NATO members), as well as uncertainty on whether this fell within ENISA's mandate. In the open public consultation, civil-military cooperation was among the needs least frequently selected by respondents (see Figure 53).

In terms of needs and opportunities, several other international bodies were mentioned as interesting for further collaboration in the future. Apart from the discussion above regarding NATO, the interviews with ENISA's various stakeholders indicated good opportunities for increased collaboration with several international bodies, for example: UN / ITU (brings on-board the poorer countries lacking means to deal with cybersecurity problems), third country governments (exportation of European model legislation, as has been done already for Japan and Qatar), the FIRST community, standard developing organisations (e.g. NIST or similar bodies at international level, the European Telecommunications Standards Institute (ETSI) and the Organisation for the Advancement of Structured Information Standards (OASIS)), Europol and Interpol (as cybercrime and security threats are often closely related).

ENISA needs to be more clearly positioned as the focal point of cybersecurity in Europe and a natural contact point for international collaboration. As presented in section3.2.2.4, ENISA is not widely described as a centre of expertise or as a reference point for stakeholders in the NIS area, mainly due to little visibility and lacking expertise in certain technical fields. Additionally, interviews with direct stakeholders indicated that a clarification with respect to international collaboration in ENISA's future mandate would be useful. It is natural, given ENISA's name, that international actors perceive ENISA as the Single Point of Contact of cybersecurity in Europe and contact the Agency to discuss cybersecurity matters and international cooperation. However, according to one of ENISA's direct stakeholders, it is not clear whether this falls within their current mandate.

3.3.7   ENISA's future mission, tasks, working practices or activities

> **EQ42: Could ENISA's mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape or would another EU initiative be more efficient?**
> Although the broad scope of the current mandate was seen as adequate by given stakeholders, others saw a need for more clarity with respect to the activities to be performed. Many direct stakeholders, advisors and users linked the limited resources of the Agency to a need for a clearer mandate, with the work being more focused on key priorities. Furthermore, there was also broad consensus that ENISA needs to develop its in-house expertise in key areas. The difficulties faced by ENISA in recruiting competent staff were identified as a key barrier to its development in this regard. No other EU initiatives were identified as being more efficient or effective than ENISA in responding to the new cybersecurity landscape but open public consultation respondents pointed to other potential EU initiatives that could complement ENISA's work in the field of cybersecurity.

Many of ENISA's stakeholders would like a revision of the mandate, with clarifications of the field of actions and key priorities. Stakeholders have different views on whether the mandate of ENISA needs to be changed or not to reflect new needs posed by the evolving cybersecurity landscape. Some of the interviewed direct stakeholders, as well as users and advisors of ENISA, think that the current mandate is wide enough (or flexible enough) to cover evolving needs, while other stakeholders think that there are some limitations to the current mandate, e.g. related to uncertainty of which actions ENISA can take to meet the needs from its users and regarding a change towards a more operational role of the Agency. As already pointed out (see e.g. section 3.2.2.8) the size of the Agency is assessed as a weakness by a close majority of surveyed stakeholders[94]. This point is confirmed by the interviews in terms of frequent requests for more resources, particularly from ENISA's direct stakeholders. Linked to the comments on ENISA's limited resources numerous interviewees (including Member States) also call for a clearer mandate and better definition of key priorities.[95] A few interviewees also see a need for an improved description of ENISA's role compared both to other EU agencies (particularly EC3 and CERT-EU) and national cybersecurity agencies. Examples of issues proposed to be clarified or to be specifically mentioned in the mandate are: the Agency's role in cyber crisis collaboration and support activities for the private.

There seems to be a general consensus among the stakeholders that ENISA needs to develop its in-house expertise in key areas. In relation to the need for more staff and greater focus on key priorities, the interviewed stakeholders (both direct stakeholder and users and advisors) see a need for ENISA to develop its expertise and concentrate its resources on fewer projects. The problems identified (see e.g. section 3.2.2.8) in attracting and retaining competent staff, particularly senior experts and technical experts, are reported as a barrier in this sense, together with the need for a revision of the current recruitment procedures. A few direct stakeholders propose increased interaction and knowledge sharing with Member States cybersecurity and NIS experts to increase the competencies of ENISA's staff. This latter approach is in line with the results of the CSIRT survey, as increased interaction between ENISA and CSIRT, together with more training activities, were seen as particularly important by respondents.

While respondents to the open public consultation pointed to other EU initiatives to help respond to current gaps and needs, these were not seen as alternatives to ENISA. Open public consultation respondents were asked to propose what other, if any, EU initiatives could be

---

[94] This refers to the "ENISA survey".

[95] This is in line with previous evaluations key explanations to some of the shortcomings regarding effectiveness, namely 1) the broad mandate and the variety of tasks it seeks to fulfil, and 2) issues with staff recruitment and limited resources.

put in place to address the gaps and needs identified (see section 3.3.1). In total, 38 respondents commented on what these other EU initiatives could be:

- National authority respondents felt that other EU initiatives could focus on "increased funding for capacity building and joint operational ventures, particularly for smaller Member States" and "further financial programmes to support CSIRTs capabilities and SMEs protection". For this, ENISA should be allowed to participate in funding programmes to ensure more effective work with Member States and to extend the range of activities it offers.

- Respondents from private enterprises and business associations commented on various topics: Specifically on the NIS Directive, a few respondents felt the current legislation was already outdated before the implementation process had been completed in Member States; therefore a revision of the Directive was considered necessary. One respondent proposed to adopt an EU-wide implementation of the US NIST framework which provides flexible and cost-effective risk based approaches and supply chain resilience, and suggested that its implementation would enable to streamline best practices across all sectors. Other contributions showed strong support for the EU to invest more in addressing the cyber skills gap ranging from basic education to professional qualification and advanced training of skilled and specialised cyber experts.

- Respondents from the other stakeholder groups agreed that there must be an approach to legislation, particularly since the "slightly chaotic process surrounding the launch and subsequent debate on the NIS Directive". Additional laws were not seen as necessary, but rather "effective continuous action" by focusing on education and information sharing at a fast pace. Other respondents also saw the need for the "establishment of a dedicated funding or financial programme for cybersecurity research", suggesting it as a "powerful incentive for government, universities and the private sector to help archive security goals".

3.3.8 Conclusions on ENISA's SWOTs

In the context of the rapid evolution of the technological landscape and the related intensification of cybersecurity threats, increased cooperation between different authorities and communities (public and private), increased capacities at Member States level and further research into cybersecurity challenges, were identified as particularly important needs. Overall, if sufficiently mandated and resourced, ENISA was considered to be able to contribute to addressing the evolving needs of the NIS domain.

On the **strengths** side, taking into account the borderless nature of cyber-attacks, as well as the concerns Member States have in disclosing sensitive information, ENISA is a neutral facilitator with policy expertise in the domain of cybersecurity.[96] The Agency is well placed to help Member States and EU institutions find common ground for agreement in the face of divergent priorities, and strengthen the levels of cooperation and collaboration among them. As noted by s noted by all of the consulted stakeholder groups and in the reviewed documentation[97], cyber resilience is a key element in the cybersecurity domain, and thus ENISA's central role in strengthening cyber resilience, by helping Member States to foster their capability and capacity development, has been identified as one of the Agency's strongest assets. The prompt eruption of new vulnerabilities and the difficulty to mitigate the attacks point to the need to involve different kinds of stakeholders in order to present a more comprehensive approach. ENISA has extensive experience engaging with different types of stakeholders which, combined with its expertise in collecting and sharing pan-

---

[96] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0.; See ENISA (2015). CYBER 7: Seven messages to the edge of Cyber-Space; Catalogue Number: TP-04-15-745-EN-C; ISB: 978-92-9204-133-5. And Largely confirmed by ENISA stakeholder interviews.

[97] See, for example European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry; Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

European data, can facilitate the identification and dissemination of best practices to overcome diverse challenges.[98]

ENISA is faced with several **weaknesses** that affect its role and effectiveness in the European cybersecurity landscape. ENISA has limited visibility in the press, media and among the general public due to weak communication and marketing, as well as limited self-assertion, meaning that its voice is only softly heard in the EU's diverse, fragmented cybersecurity landscape. What is more, ENISA's lacks a long-term vision as it is too constrained by its annual work programme. Aside from these substance-related challenges, there are more structural weaknesses that also have been identified in the evaluations of ENISA's activities in 2014 and 2015. ENISA lacks sufficient human and financial resources to complete its various activities to a high standard. The size of the Agency was considered by several stakeholders[99] to be insufficient to handle all the tasks entrusted to it, including the new tasks imposed by the NIS Directive. An additional burden concerns ENISA's difficulties to attract and retain qualified human resources.

The NIS Directive can be seen as an **opportunity** for ENISA to increase its role and importance in the cybersecurity landscape. In the light of increased levels of digitisation and rapidly evolving cyber-threats, ENISA could profit from growing demands for synergies between operators, e.g. digital service providers, encouraging collaboration across different sectors and stakeholders concerned or affected by cybersecurity policies. According to several industry representatives, one area of great potential for ENISA concerns the introduction of ICT standardisation and certification with a view to supporting further integration of the Single Market and consumer trust.[100] In addition, ENISA's users and advisors agree that there is an acknowledged need and demand for awareness raising in the field of cybersecurity and ENISA could have a strong role in coordinating future action in this regard.

From a formative, future-oriented perspective, ENISA is faced with several **threats** that impact on the cybersecurity context in which the Agency is operating. Attacks are not only becoming more sophisticated, but are also more pervasive. The rapidly changing landscape, in addition to the growth in the interconnectivity of devices, have been recognised in several studies[101] [102] as contributors to the prompt eruption of new vulnerabilities and difficulties in mitigating attacks. A lack of capacity to meet such rapidly changing threats is considered an important threat faced by ENISA. Furthermore, ENISA is dominated by Member States' divergent priorities and capabilities. Since Member States have difficulties agreeing on common action in ENISA, the outcome is often the least threatening action to all Member States. This in turn is limiting ENISA's scope of action.[101] A further contextual threat concerns the general fragmentation of EU cybersecurity policy with several, at times competing, agencies active in the cyber-policy domain. Last but not least, there is a recognised lack of trained experts in cybersecurity in Europe which aggravates the Agency's recruitment difficulties.[103]

The table in Appendix 5 presents a more comprehensive compilation of ENISA's SWOTs, while Figure 59 below summarizes the main SWOTs identified.

---

[98] European Commission (2013). JOIN (2013) 1 final: 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: An Open, Safe and Secure Cyberspace.

[99] Findings from the ENISA survey as well as from stakeholder interviews

[100] See interviews; the proposal for further action equally appears in: See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

[101] Accenture and HfS Research (2016). The State of Cybersecurity and Digital Trust 2016.

[102] EY (2015). Cybersecurity and the Internet of Things.

[103] Finding from ENISA stakeholder interviews.

Figure 59: ENISA's main SWOTs

Strengths	Weaknesses
- Neutral, facilitator, free of political bias or commercial interests - Recognised support to Member States in capacity building & capability development to strengthen resilience to cyber-threats - Acknowledged collaboration & community building reaching wide range of actors, incl. Member States, industry, EU bodies etc. - Horizontal expertise, "landscape overview" of Member States cybersecurity policies	- Low visibility for various reasons: Lack of expertise, weak communication/marketing and limited self-assertion within the EU cybersecurity policy landscape - Lack of a long-term, strategic vision - Recruitment difficulties - Reduced efficiency due to split location - Distance to EU decision makers in Brussels - Lack of financial and human resources to make a difference
Opportunities	**Threats**
- Growing need for synergies between ICT operators to ensure concerted and collaborative NIS policy actions - NIS Directive bears the potential to strengthen ENISA's role in EU cybersecurity policy - There is an acknowledged need and demand of stakeholders to strengthen awareness raising of cybersecurity - Stronger support in the community is evolving for ICT standardisation and certification	- Policy fragmentation at EU level and diverging policy priorities in EU Member States constrain ENISA's scope of action - Rapidly evolving and complex threat landscape involving multiple disciplines create new vulnerabilities, e.g. IoT - Lack of overall (technical) talent in the field of cybersecurity aggravates ENISA's recruitment difficulties

4. CONCLUSIONS AND RECOMMENDATIONS

On the basis of the findings presented above, this section presents overall conclusions on the successes of ENISA and the most pressing issues that need to be addressed in order to ensure a coherent approach to NIS in Europe in the future. These issues are situated at the more strategic, policy level and at the level of ENISA as the subject of this study and one of the current players in this sphere. Following on from these, a series of possible options to review the current mandate of ENISA have been presented, including an assessment the costs of each of these options, their potential EU added value and their impact on ENISA's coherence with national and EU cybersecurity bodies.

4.1 Successes of ENISA

Over the 13 years of its existence ENISA has made some important achievements towards increasing NIS in the EU. The main successes of ENISA, identified on the basis of the findings and conclusions of this evaluation study are presented below.

ENISA implements activities and provides services in an area of rapidly increasing relevance. The increased frequency, sophistication and potential impact of cyber-threats shows the need for a coordinated approach across the EU. This is where ENISA's objectives to contribute to securing NIS in Europe through the provision of expertise, increasing capacities, fostering cooperation and supporting the development and implementation of legislation and policies is of high relevance. Overall, if sufficiently mandated and resourced, ENISA was considered to be able to contribute to addressing the evolving needs of the NIS domain.

ENISA has contributed to building a community of cybersecurity stakeholders across the EU. ENISA has proven capable of maintaining a viable network with a range of different stakeholders comprising national authorities, the EU institutions and bodies, academia, civil society organisations and to some extent also the private sector. ENISA is perceived as a trusted partner and acts as a node between the different organisations to gather and exchange information and best practices among Member States and beyond. A main success is the establishment of the a network of CERT/CSIRT which benefitted from training and workshops thereby fostering coordination and exchange.

ENISA's has increased capacity and coordination on cyber-attacks in the EU. In particular with the cyber exercises ENISA has brought together public and private stakeholders to increase their understanding of and capacities in NIS. As one of the Commission representatives pointed out in the context of the study, following the recent attack of multiple variants of a ransomware named WannaCry which affected many organisations in the European Union, ENISA successfully ensured cyber cooperation at EU level for the first time[104]. Other capacity building activities, such as trainings and the provision of manuals further contribute to better prevention, detection and response to incidents across the EU.

ENISA makes NIS knowledge available and accessible. Some of ENISA's publications have been highly appreciated and are considered to be very useful. ENISA's publications provide relevant information on cybersecurity issues from an EU-wide perspective. The publications present technical expertise in a language that is accessible to policy makers and a broader public. Publications that were specifically highlighted by stakeholders as contributing to the study cover

---

[104] See also: ENISA's press release on the issue. Available at: https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level

issues such as incident reporting, cloud computing and crisis management. ENISA's neutrality as a decentralised EU agency is appreciated by the public and private sector.

Finally, ENISA has contributed to increasing awareness about cybersecurity across the EU through the cybersecurity month. While the activities are increasingly organised by Member States with more independence from ENISA, the Agency has contributed to setting up this activity which reaches public and private stakeholders, as well as citizens across the EU with the aim of increasing their understanding of the risks posed to NIS.

ENISA efficiently implements its assigned tasks. ENISA's staff are highly dedicated to their work and ensure that despite tight resources, planned outputs are delivered. Within the Agency efficient work processes have been established with a clear delineation of responsibilities.

4.2   Most pressing issues at the strategic / policy level

The most pressing issues that need to be addressed in order to ensure a coherent approach to cybersecurity in Europe on the basis of the findings and conclusions of this study are presented below.

Cybersecurity at the EU institutional level is fragmented: There are a number of EU-level actors that are active in the cybersecurity area including ENISA, CERT-EU and EC3 (Europol), leading to a fragmented approach towards cybersecurity among EU institutions. There is no one central point of reference for cybersecurity in Europe. While the mandates of these organisations are in theory different, their roles are not clearly defined in practice and there is a potential for overlap, as the positioning exercise presented in section 3.2.4.3 points to. Within this context, ENISA has had difficulty carving out a place for itself and has found other organisations such as CERT-EU in particular filling a gap by carrying out activities that would from a legal perspective fall within ENISA's remit.

The institutional and legal framework for cybersecurity in Europe is rather weak: Cybersecurity has not been seen as a legal priority at EU-level until more recently. The Single Market acquis[105] do not apply to digital services to the same extent as to other areas. This has had an impact on the degree to which cross border cooperation in relation to NIS is working. Cybersecurity is primarily an area of national competence, while in reality it is an issue that transcends borders; an effective strategy for the prevention, mitigation and response to cyber threats/attacks requires cooperation across Member States. The advent of the NIS Directive, the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (COM(2016) 410), and the priorities set by the Digital Single Market Strategy (COM(2015) 192) represent key new pillars to strengthening the institutional and legal framework for cybersecurity in Europe going forward.

4.3   Most pressing issues at the ENISA level

At the level of ENISA, the study's findings point to a series of issues that would need to be addressed in order for the Agency to play a key role in cybersecurity in Europe going forward.

ENISA lacks visibility: ENISA has not been able to carve out a strong, clear place for itself within the European cybersecurity landscape. While it is known and recognised within its circle of stakeholders, it has not managed to develop a strong brand name or be seen as the one point of reference at European level for cybersecurity. A number of factors help to explain this, including the fragmented nature of cybersecurity in Europe with multiple actors seeking to position

---

[105] http://ec.europa.eu/internal_market/copyright/acquis/index_en.htm

themselves within the areas of prevention, mitigation and response. Finally, the degree to which ENISA has been "allowed in" and consulted by the Commission and other players acting at EU level in this field has impacted on its visibility. While ENISA is more frequently consulted than in the past, it is not necessarily present in all relevant fora dealing with or funding programmes (e.g. CEF) related to cybersecurity at European level.

ENISA does not have sufficient financial or human resources at its disposal to effectively respond to its broad mandate: Despite evolutions over the past few years in the degree of importance of cybersecurity and an according increase in the scope of ENISA's mandate, ENISA's budget has remained very limited. With the advent of the NIS Directive and the new tasks entrusted to it, e.g. taking part in the Cooperation Group and acting as the secretariat for the CSIRT Network, it has also had to prioritise and set aside some of the areas it has previously focussed on, thereby further depleting resources. While the evaluation suggests that there is potential for ENISA to increase its efficiency by introducing more flexibility in their programming cycle or automatization of some of the administrative processes, such improvements would not be sufficient in their scope to allow it to effectively respond to its broad mandate. An important area for improvement is recruitment. ENISA has difficulty recruiting and retaining the staff required for it to have the necessary expertise at its disposal to perform tasks in-house and in some cases to the quality standards expected (i.e. reference was made by stakeholders to the varying levels of quality of ENISA reports/publications in particular). This is due to both internal (i.e. slow recruitment procedures in a fast-paced, competitive environment; a lack of career progression prospects) and external factors (i.e. small budget; constraining staff management rules (e.g. number of CAs versus TAs); an expertise shortfall in the sector; and a lack of competitive salaries in an area that is dominated by demand from the private sector.

ENISA is not perceived as a proactive, visionary Agency: ENISA's mandate is broad enough to be all encompassing and allows for flexibility in the tasks it carries out. This leads to it being reactive by seeking to fulfil needs of as many stakeholders as possible and not being focussed, proactive and visionary. Stakeholders suggested that increased expertise within the Agency and a stronger focus on research could allow for ENISA to be more abreast of developments in cybersecurity. To make use of this knowledge, ENISA would need to be able to be more flexible in setting its own work priorities. One of the factors explaining this is the Member State dominance (via the Management Board) of the work programme. Given the differing needs and priorities of Member States, there is not a common line among Member States and the work programme tends to lead to ENISA having work priorities that represent the lowest common denominator among Member States and are not perceived as threatening to the national competence of given Member States. As such, ENISA has a tendency to spread itself too thin, as also concluded in the 2015 evaluation.

There is little consensus on what the future role of the Agency should be: The divergent needs of ENISA's stakeholders lead to a lack of consensus on whether the Agency should take on a more operational role, or continue to be an Agency acting solely at the strategic level. In taking on a more operational role, it could gather data, monitor and share information on incidents occurring throughout the EU in order to ensure increased transparency and enable Member States to coordinate joint responses to incidents where this proves necessary. While Member States with fewer resources at their disposal and industry would perceive this as a positive development, Member States with strong cybersecurity capacity tend to see it as an encroachment on their area of national competence.

4.4 Options for the future

Table 26 below sets out a set of possible options to review the current mandate of ENISA, including the issues that they would seek to address and expected results of the different factors for change that could be considered under each option. It also presents an assessment of the added value of each of the new changes foreseen and of the risk of overlap with the tasks and activities of other national, European or international bodies. The third table provides an estimation of the costs related to each of the factors for change derived from the results of the evaluation; these are based on a series of assumptions, as presented in the table.

The section therefore serves to respond to the evaluation questions presented below.

Table 25: Evaluation questions on the options for the future of ENISA

Prospective EQ43: What would be the financial implications associated with each of the possible options for modifying ENISA's mandate as they emerge from the evaluation? EQ44: If any new tasks for ENISA are identified (e.g. through EQ4 and EQ37), do these represent EU added value? EQ 45: Taking into account the new tasks (identified during the evaluation), will there be any risk of ENISA's tasks and activities overlapping with those of other national, European or international bodies?

Table 26: Options for the future – the key issues they will address and expected results

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
Option 0: Baseline, maintain the status quo **This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation and Telecoms Framework Directive would need to be taken into account.**	N/A as status quo	**Revise ENISA's mandate to make its new tasks as per recent/upcoming legislation more specific:** • **Involvement in Cooperation Group:** Support MS cooperation on drafting and maintaining over time voluntary guidelines on security measures • **CSIRT Network Secretariat:** Provide technical support for back-end services that enable CSIRTs to exchange information on best practices	Continuation of status quo If factor for change is implemented (review of mandate in light of new tasks) – Increased coherence of ENISA's mandate and thus activities with EU cybersecurity policies	N/A as status quo (see section 3.2.4.5 and section 3.2.5.1)

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
		and actual incidents and threats, as well as support voluntary cooperation in case of incidents • **Electronic communications code, recital 92**: Contribute to an enhanced level of security of electronic communications by, amongst other things, providing expertise and advice, and promoting the exchange of best practices • **eIDAS**: (1) Recital 39 - Enable the EC and MSs to assess the effectiveness of the breach notification mechanism introduced by this Regulation by, for example, aggregating the national reports provided by supervisory bodies into an annual Report on EU Breaches in Trust Service Providers. (2) Support supervisory authorities in the drafting and supervision of security measures of Trust Services through, for example, supporting national regulators in the drafting and maintenance of guidelines on security measures and incident notification formats and procedures on Trust Services		
Option 1: Expiry of ENISA mandate (terminating ENISA) **This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under,**		N/A	See section 3.2.5.3	N/A

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
for example, the NIS Directive and bilateral or regional ties at Member State level.				
Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate) **This option concerns making significant revisions to ENISA's mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.**	The current level of cyber threats in the EU requires an enhanced, coordinated approach Member States with fewer cybersecurity capacities need support to prevent, mitigate and respond to cybersecurity threats ENISA is not perceived as a proactive, visionary agency	**Strengthen ENISA's operational role:** • **Provide periodic threat intelligence and ad hoc alerts**: ENISA would develop and maintain its own threat intelligence capacity in order to monitor the threat landscape and provide MSs fast alerts/warnings on emerging threats and risks and monitor security incidents, including those affecting specific MSs. This would involve: (1) producing regular threat intelligence reports including high-level strategic analyses on threats, incidents and trends (e.g. key technological developments) and (2) collecting and analysing public communications on an event and compiling EU-level flash reports and guidance to businesses and citizens. • **Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level**: ENISA would: (1) organise cybersecurity exercises to test the Blueprint at all levels – operational, tactical and strategic) with all stakeholders; (2) collect and aggregate reports from national sources (CSIRTs) to establish a common situation awareness report for decision	Based on information shared by the Member States, ENISA will be able to provide a common baseline and up-to-date threat analysis The Agency will ensure cooperation and coordination across the Member States in case of an incident concerning several Member States ENISA would support capacity building in Member States through the provision of technical assistance on an on-demand basis ENISA will further assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents	<u>EU added value of new tasks:</u> These tasks aimed at strengthening ENISA's operational role represent EU added value as there is a need for data to be gathered <u>at EU level</u> to provide a common baseline and up-to-date threat analysis in order to share knowledge, foment cooperation among Member States and help better respond to cyber security incidents that are cross-border in their nature There is also a need for capacity to be increased, in particular among smaller Member States that tend to invest fewer resources in cyber security, through the exchange of knowledge and expertise <u>at EU level</u> <u>Coherence with tasks of other bodies:</u> With a strengthened operational role foreseen for ENISA there will be a need to clarify the respective roles of other EU bodies active in the area and which have been seeking to fill a vacuum in some of these areas (e.g. CERT-EU), as well as increase coordination between them

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
		makers in the event of an incident; (3) support technical handling of the incident, including facilitating sharing of technical solutions between MSs; (4) handle public communication around the incident; (5) in case of a major crisis, propose the activation of the political decision making (IPCR) by alerting all or one of the EU institutions; (6) publish flash report or alerts in the event of significant events or incidents based on publically available information OR information made available through the CSIRT Network • **Provide emergency cybersecurity response**: ENISA would provide on-demand technical assistance to MS bodies and institutions by creating and maintaining a team of experienced senior cybersecurity incident advisors who may be sent to MSs upon their request to assist and contribute to cybersecurity incident response and recovery		
	The institutional and legal framework for cyber security in Europe is rather weak The current level of cyber threats in the EU requires an enhanced, coordinated	**Strengthen ENISA's role in policy development and implementation:** • Establish ENISA as an agency that has to be involved by other EU bodies, including the Commission, when cybersecurity matters are being considered • Formally involve ENISA in the implementation of the Connecting Europe Facility on	ENISA will play a stronger role in assisting the Union institutions, bodies, offices and agencies and Member States in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to a	EU added value of new tasks: These tasks aimed at strengthening ENISA's role in policy development and implementation represent EU added value in that this policy development is happening at the EU level and ENISA has a cross-Member State perspective on cyber security on the basis of the multi-stakeholder network it has managed to establish and can draw on

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	approach ENISA lacks the visibility required to ensure it is seen as a key player and called upon to play an active role in EU policy making on cybersecurity	Telecom as an advisory body • Establish semi-formal governance structures with regular meetings between ENISA and other agencies/international organisations (e.g. on given common themes such as training) to increase cooperation at EU institutional level Increase ENISA's visibility: • Set-up a liaison office in Brussels with two to three permanent employees • Create a dedicated communications team within ENISA	less fragmented, more coherent legal and institutional framework and ultimately the proper functioning of the internal market ENISA will be able to more easily and cost-effectively ensure a presence in Brussels and build awareness, notably when it comes to its strengthened role in policy development and implementation, but also in relation to research and innovation EU institutions and bodies will benefit from ENISA's input on cybersecurity EU institutions and bodies, Member States and other stakeholders will be more aware of the expertise and support available through ENISA	Coherence with tasks of other bodies: Increasing ENISA's involvement in policy development and implementation will imply the Agency increasing its ties and involvement with other bodies active in the area, thereby increasing the potential for synergies to be developed
	The institutional and legal framework for cyber security in Europe is rather weak There is limited long-term planning for ENISA's activities	**Make ENISA's mandate permanent:** • This would involve ENISA having a permanent mandate, but still allow for the periodic evaluation of the performance of the Agency	ENISA will be put on the map, ensuring a more permanent presence and longer-term, strategic outlook Will lead to an increase in staff retention, planning and competence development by providing a more long term perspective	EU added value of new tasks: N/A Coherence with tasks of other bodies: N/A
	ENISA's work programme is dominated by the interests of Member	**Strengthen ENISA's governance structure:** • Formally involve other stakeholders in the	ENISA will be less Member State dominated, thereby leading to a work programme that takes into	EU added value of new tasks: N

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	States	governance of ENISA by increasing the weight of the PSG in playing an advisory role on ENISA's Work Programme • Allow more flexibility for ENISA to determine its own work priorities at Executive Board level	account the needs of a variety of stakeholders including those of the EU institutions and the private sector The Agency will use its expertise to stimulate further cooperation between actors from the public and private sector The needs of the private sector will be better addressed	Coherence with tasks of other bodies: N/A
	There is a need for EU level coordination on standardisation and certification of ICT	**Include a role for ENISA in EU-level standardisation and certification:** • **Support the EU ICT Security Certification Framework**: Put in place an EU ICT security certification framework whereby ENISA would play a supporting role by (1) providing the secretariat and actively supporting the work undertaken (e.g. convene meetings of the framework's governance structures and meetings and engagements with industry stakeholders);(2) providing technical expertise to Member States (e.g. MS taking part in the framework on issues related to security testing and vulnerabilities in ICT products); and (3) compiling and publishing guidelines concerning the security requirements of ICT products and services in cooperation with national authorities and	Standardisation will be further supported ENISA would support capacity building in the Member States through the provision of technical expertise	EU added value of new tasks: These tasks aimed at strengthening ENISA's role in standardisation and certification represent EU added value in that action in this area needs to take place at a cross-European level and ENISA, with its wide network of EU-level stakeholders, demonstrated ability as a neutral player to support cooperation across Member States and stakeholders with differing views and its ability to compile and report on technical issues, will be key in ensuring this Coherence with tasks of other bodies: In performing these tasks, ENISA will draw on existing sources to come up with assessments and guidelines and fill a void in this area at EU level. There is therefore limited risk of overlap of its activities in this area with other bodies at EU and international level. At national level, there is a risk of duplication of efforts where given Member States make their own recommendations/provide guidelines in this area.

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
		industry, thereby communicating the work of the framework to industry, consumers at EU and international level • **Support ICT security standardisation**: ENISA would provide a supportive role in facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services, including by cooperating with Member States on technical areas concerning the security requirements for operators of essential services and digital service providers. This could involve supporting the work of the EU ICT Security Certification Framework in EU and international standard organisations; taking part in and contributing to the work of cybersecurity working groups of the European Standardisation Organisations (ESCs); performing reviews and assessments of cybersecurity related standards when associated with regulatory and legal requirements (e.g. eIDAS)		
	Cyber security at the EU institutional level is fragmented ENISA is not perceived as a proactive, visionary Agency	**Strengthen ENISA's position relative to research and innovation:** • **Take part in programming implementation**: ENISA would implement parts of the Framework Programme for R&I which relates to	Research and development will be further supported ENISA's presence in this area will be strengthened, thereby increasing its visibility and its access to information on latest technological	EU added value: These tasks aimed at strengthening ENISA's position relative to R&I represent EU added value in that ENISA has a cross-Member State perspective on what is going on in the cyber security field on the basis of the multi-stakeholder network it has

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
	ENISA lacks the visibility required to ensure it is seen as a key player and called upon to play an active role in contributing to research and innovation	cybersecurity whereby the EC delegates the relevant powers by performing the following tasks: (1) managing some stages of the programme implementation and some phases in the lifetime of specific projects on the basis of WPs adopted by the EC; (2) adopting the instruments of budget execution for revenue and expenditure and carrying out all the operations necessary for the management of the programme; and (3) providing support in programme implementation. Examples of the activities ENISA could perform include implementing calls on Public Procurement of Innovation (PPI) in close collaboration with MS authorities, and supporting MS public procurers in identifying common research and innovation requirements • **Take part in programming through playing an advisory role:** ENISA would play an expert advisory role in the cyber security-related elements of EU R&D funding programmes (H2020, CEF) by sitting on an advisory committee, providing independent advice and input and feeding into ideas for research. • **Benefit from EU R&I funding**: Open ENISA's mandate to take part in EU R&D funding programmes (H2020, CEF) as a recipient of	developments	managed to establish and can draw on Coherence with tasks of other bodies: By taking part in programming implementation, ENISA would take on a series of tasks currently implemented by the European Commission, thereby ensuring a lack of overlap. Moreover, there is no other cyber security-focussed body at EU level involved in advising at programme level.

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
		funding by changing the provisions on source of revenue but not adding it as a task. ENISA can provide added value to industry and academia in R&I by leveraging its practical expertise in areas such as cooperation, information sharing and regulatory requirements. *Note: Either one or the other options set out above could be pursued due to issues of conflict of interest.*		
Option 3: European Agency with full operational capabilities (Establish a European Centre of Cybersecurity) **This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.**	Cyber security at the EU institutional level is fragmented The current level of cyber threats in the EU requires an enhanced, coordinated approach	**Create an EU level cyber security umbrella:** • Develop an umbrella organisation covering ENISA and CERT-EU, thereby bringing together three main functions, namely policy advice, centre for information and Computer Emergency Response Team. The operational role of CERT-EU in responding to cyber incidents in the EU institutions would therefore be combined with ENISA's role of ensuring cooperation in the event of an incident. The new organisation would act as an EU contact point for cybersecurity related issues in close coordination with the EEAS. Options include merging ENISA and CERT-EU and having a governance structure that would allow different reporting lines and oversight for the team dealing with the EU institutions, or integrating (part of) CERT-EU within ENISA as one of the	A more coordinated response to cyber incidents would be ensured across the EU and its various players Member States would receive direct support when responding to cyber incidents	EU added value of new tasks: N/A Coherence with tasks of other bodies: The potential for overlap between ENISA's work and that of CERT-EU would be avoided

Options	Key issues to address	Factors of change	Expected results	Assessment of EU added value (EQ44) and coherence (EQ 45)
		Agency's departments.		
	Cyber security at the EU institutional level is fragmented The current level of cyber threats in the EU requires an enhanced, coordinated approach ENISA is not perceived as a proactive, visionary Agency	**Create a virtual European CSIRT**: • **Coordinate CSIRT Network operations**: Enable the Agency to coordinate the operations of MS CSIRTs, collecting information and pooling national resources on analysing threats and responding to incidents • **Produce real time situational awareness and dynamic (live) threat intelligence feeds**: Enable ENISA to act as a broker, sharing information on incidents between Member States in the form of real-time situational awareness and dynamic (live) threat intelligence feeds on the basis of information exchanged on the CSIRT Network • **Maintain and provide own cybersecurity incident response capacity to public and private sector**: ENISA would create and maintain the capacity to provide on-demand technical operational assistance to MS CSIRTs, operators of essential services, EU bodies and institutions for the prevention, detection and response to incidents	Creation of a more coherent, stronger CS presence in Europe Based on information shared by the Member States, ENISA will be able to provide a real time threat analysis The European CSIRT will ensure cooperation and coordination across the Member States in case of an incident concerning several Member States The European CSIRT would support capacity building on an on-demand basis in the public and private sector The European CSIRT would further assist the Union and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents	EU added value: These tasks aimed at creating a virtual European CSIRT represent EU added value as there is a need for real-time data to be gathered, assessed and shared at EU level to provide common, real-time situational awareness and dynamic (live) threat intelligence, foment cooperation among Member States and help better respond to cyber security incidents that are cross-border in their nature There is also a need for capacity to be increased, in particular among smaller Member States that tend to invest fewer resources in cyber security, through the exchange of knowledge and expertise at EU level Coherence with tasks of other bodies: Such a body aimed at providing response services to stakeholders other than EU institutions, agencies and bodies does not currently exist at EU level. However, if such a body were created independently of CERT-EU, there would be a need to clarify the respective roles of other EU bodies active in the area and which have been seeking to fill a vacuum in some of these areas (e.g. CERT-EU), as well as increase coordination between them
	As above	All factors related to Option 2 would/could be fulfilled under Option 3 as well	As above	As above

4.5   Costs of the options

This section provides an estimation of the costs related to each of the factors for change derived from the results of the evaluation of ENISA. The estimations are presented in two tables: The first table (Table 27) provides an **overview of the estimated costs per option and per grouped factors of change**. It should be read in combination with the second table (Table 28) which provides more **detail on the costs per factor of change** and the **specific assumptions** applicable to the estimations of each of the individual cost factors.

The costs are based on a series of **general assumptions**:
- It has been assumed that the Greek government will continue to provide its current financial contribution (of EUR 640,000 per year) for the offices in Heraklion and Athens.
- It has been assumed that Temporary Agents (TAs) would implement the new tasks foreseen and averages of the salaries (as per Article 66 of the Staff Regulations, applicable from 1 July 2016) of categories of TAs minus the 79.3% corrective coefficient for Greece have been applied as follows: Junior experts/analysts (grades AD5 to 6 – EUR 4,214/month, equivalent to EUR 50,568/year), Senior experts/analysts (grades AD7 to 12 – EUR 7,046/month, equivalent to EUR 84,552/year) and Heads of Unit (grades AD9 to 14 – EUR 9,020/month, equivalent to EUR 108,240/year). For staff based in Brussels, no coefficient applies.
- For the calculation of overall costs per option, efforts have been made to take potential synergies between the different factors for change listed under each option into account. However, it can be expected that there are further synergies to be gained should ENISA be changed to take into account all the factors for change listed under Options 2 and 3 in the evaluation study report.
- Additional set-up costs could apply, for example, for staff recruitment; these have not been taken into account here.

The cost estimations are based on several **sources**:
- A variety of stakeholders were consulted in order to further operationalise the factors for change and establish the assumptions presented below. They included representatives of DG CONNECT, ENISA, industry and Member States.
- A number of reports and documents have been consulted, as listed in the table below.

Secondary sources
ENISA Annual Activity Report 2015.
Europaid (2017): Current per diem rates. Available at: **https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17_en.pdf**. **Accessed 16.06.2017.**
Proposal for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/20**07 and Council Decision 2005/267/EC, COM(2015) 671 final.**
Statista – The Statistics Portal (2016): Rental prices of prime office properties in selected European cities as of 4th quarter 2016 (in euros per square meter per year). Available at: **https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/**. **Accessed 16.07.2017**
ENISA (2017): Statement of estimates (budget 2017). Available at: **https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets/enisa-2017-annual-budget**. **Accessed 16.07.2017**
ENISA (2017): Programming document 2017-2019. Available at: **https://www.enisa.europa.eu/publications/corporate/enisa-programming-document-2017-2019**. **Accessed 19.06.2017**

The cost estimations for each of the four options are presented below. The table presents the costs for year 1 of the introduction of the options, including specific set-up costs where relevant (notably in Option 3). The costs of each option in the following four years are also presented, considering the costs arising once an option is fully implemented. Please note that no standard inflation rate has been applied.

Two scenarios are presented. The first one considers the minimum changes that need to be implemented under each option. Costs thus represent the minimum number of staff and additional meetings that will be needed. The second scenario presents a more ideal situation, where costs represent the staff that need to be hired and meetings to be held for a smoother implementation of the options. Under Option 1 the minimum scenario assumes that ENISA will be able to take on all new tasks assigned to it as per recent legislative changes by reallocating responsibilities and tasks, as it has been done in the 2016 and 2017 Work Programme. The second scenario assumes that ENISA will get another eight staff members (two for each of the key sectors finance, health, transport and energy) to respond to its new responsibilities.

The costs are presented differentiating between staff costs (costs due to additional human resources) and "other" costs for additional office space, meetings or operational activities. These are further explained and specified in Table 28.

Under Option 2 and 3, three sub-options are presented (a, b and c) because there are three different factors of change to strengthen ENISA's position relative to research and innovation which exclude one another due to issues of conflict of interest. Sub-option a) represents the costs for the factor of change under which ENISA will take part in programme implementation of the Framework Programme for R&I; a lump sum of EUR 3.5 m has been estimated for this factor of change based on a similar function foreseen for Frontex[106] (including additional staff) which is added under "other" costs. Sub-option b) includes the costs of ENISA taking part in programming through playing an advisory role in EU R&D funding. Sub-option c) includes the costs of ENISA befitting from EU R&I funding (which are nil).

Table 27: Cost estimations for the options –overview

	Year 1				Year 2 to 5			
	Scenario 1 – Minimum changes		Scenario 2 - Ideal changes		Scenario 1 – Minimum changes		Scenario 2 - Ideal changes	
	Costs in EUR per year	Number of staff/ specification of other costs	Costs in EUR per year	Number of staff/ specification of other costs	Costs in EUR per year	Number of staff/ specification of other costs	Costs in EUR per year	Number of staff/ specification of other costs
Option 0: Baseline, maintain the status quo: This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation and Telecoms Framework Directive would need to be taken into account.								
Current budget	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84
Revise ENISA's mandate to make its new tasks per	0	0	676,416	8 (8 senior experts)	0	0	676,416	8 (8 senior experts)

---

[106] Based on: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC, COM(2015) 671 final. See SPECIFIC OBJECTIVE NO 6 "Management of Pooled resources and R&D. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation_on_the_european_border_and_coast_guard_en.pdf

	Year 1				Year 2 to 5			
recent/upcoming legislation more specific								
Total budget under the option	**11,244,679.00**	**84** (48 TAs, 31 CAs, 5 SNEs)[107]	**11,921,095.00**	**92** (56 TAs, 31 CAs, 5 SNEs)	**11,244,679.00**	**84** (48 TAs, 31 CAs, 5 SNEs)	**11,921,095.00**	**92** (56 TAs, 31 CAs, 5 SNEs)
Option 1: Expiry of ENISA's mandate (terminating ENISA): This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive and bilateral or regional ties at Member State level.								
Current budget	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84
Costs savings for the EU budget[108]	**10,322,000.00**	**84**	**10,322,000.00**	**84**	**10,322,000 plus standard 2% increase per year**	**84**	**10,322,000 plus standard 2% increase per year**	**84**
Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate): This option concerns making significant revisions to ENISA's mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.								
Current budget	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84
Strengthen ENISA's operational role	531,000.00	6 (1 HoU, 5 senior experts)	700,104.00	8 (1 HoU, 7 senior experts)	531,000.00	6 (1 HoU, 5 senior experts)	700,104.00	8 (1 HoU, 7 senior experts)
	926,142.00	Exercises	926,142.00	Exercises	926,142.00	Exercises	926,142.00	Exercises
Strengthen ENISA's role in policy development and implementation	1,140,235.75	13 (3 HoU, 10 senior experts)	1,251,077.00	15 (3 HoU, 12 senior experts)	1,140,235.75	13 (3 HoU, 10 senior experts)	1,251,077.00	15 (3 HoU, 12 senior experts)
	175,320.00	Meetings	175,320.00	Meetings	175,320.00	Meetings	175,320.00	Meetings
	7,500.00	Office space	7,500.00	Office space	7,500.00	Office space	7,500.00	Office space
Make ENISA's mandate permanent	n/a		n/a		n/a		n/a	
Strengthen ENISA's governance structure	n/a		n/a		n/a		n/a	
Include a role for ENISA in EU-level standardisation and certification	361,896.00	4 (1 HoU, 3 senior experts)	531,000.00	6 (1 HoU, 5 senior experts)	361,896.00	4 (1 HoU, 3 senior experts)	531,000.00	6 (1 HoU, 5 senior experts)
	28,002.00	Events/ meetings	58,440.00	Events/ meetings	28,002.00	Events/ meetings	58,440.00	Events/ meetings
Strengthen ENISA's position relative to research and innovation sub-option a)	3,500,000	Total costs based on similar function in Frontex	3,500,000	Total costs based on similar function in Frontex	3,500,000	Total costs based on similar function in Frontex	3,500,000	Total costs based on similar function in Frontex
Strengthen ENISA's	192,792.00	2 (1 HoU, 1	277,344.00	3 (1 HoU, 2	192,792.00	2 (1 HoU, 1	277,344.00	3 (1 HoU, 2

[107] Based on: Multi-annual staff policy plan year 2017-2019, Establishment plan in Draft EU budget 2017, in ENISA Programming document 2017-2019; Annex III

[108] Excluding the budget contribution by Greece and other income of the Agency

	Year 1				Year 2 to 5			
position relative to		senior expert)		senior expert)		senior expert)		senior expert)
research and innovation sub-option b)	23,373.00	Meetings	35,064.00	Meetings	23,373.00	Meetings	35,064.00	Meetings
Strengthen ENISA's position relative to research and innovation sub-option c)	n/a		n/a		n/a		n/a	
Additional staff costs sub-option a)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00	29 (5HoU, 22 senior, 2 junior experts)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00	29 (5HoU, 22 senior, 2 junior experts)
Additional staff costs sub-option b)	2,225,923.75	25 (6 HoU, 18 senior, 1 junior expert)	2,759,525.00	32 (6 HoU, 24 senior, 2 junior experts)	2,225,923.75	25 (6 HoU, 18 senior, 1 junior expert)	2,759,525.00	32 (6 HoU, 24 senior, 2 junior experts)
Additional staff costs sub-option c)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00	29 (5HoU, 22 senior, 2 junior experts)	2,033,131.75	23 (5 HoU, 17 senior, 1 junior experts)	2,482,181.00	29 (5HoU, 22 senior, 2 junior experts)
Additional other costs sub-option a)	4,636,964.00		4,667,402.00		4,636,964.00		4,667,402.00	
Additional other costs sub-option b)	1,160,337.00		1,202,466.00		1,160,337.00		1,202,466.00	
Additional other costs sub-option c)	1,136,964.00		1,167,402.00		1,136,964.00		1,167,402.00	
Total budget under the sub-option a)	**17,914,774.75**	**107**	**18,394,262.00**	**113**	**17,914,774.75**	**107**	**18,394,262.00**	**113**
Total budget under the sub-option b)	**14,630,939.75**	**109**	**15,206,670.00**	**116**	**14,630,939.75**	**109**	**15,206,670.00**	**116**
Total budget under the sub-option c)	**14,414,774.75**	**107**	**14,894,262.00**	**113**	**14,414,774.75**	**107**	**14,894,262.00**	**113**

	Year 1				Year 2 to 5			
Option 3: European Agency with full operational capabilities (Establish a European Centre of Cybersecurity): This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.								
Current budget	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84	11,244,679.00	84
Create an EU level cybersecurity umbrella	243,125.75	2 (1 HoU, 1 senior expert)	349,753.00	3 (1 HoU, 2 senior experts)	243,125.75	2 (1 HoU, 1 senior expert)	349,753.00	3 (1 HoU, 2 senior experst)
	7,500.00	Office space	7,500.00	Office space	7,500.00	Office space	7,500.00	Office space
Create a virtual European CSIRT	2,531,104.00	29 (3 HoU, 26 senior experts)	3,446,448.00	40 (3 HoU, 37 senior experts)	361,896.00	39 (3 HoU, 36 senior experts)	446,448.00	91 (3 HoU, 88 senior experts)
Additional staff costs	2,774,229.75	31 (4 HoU, 27 senior experts)	3,796,201.00	43 (4 HoU, 39 senior experts)	3,651,469.75	41 (4 HoU, 37 senior experts)	8,127,201.00	94 (4 HoU, 90 senior experts)
Additional other costs	7,500.00		7,500.00		7,500.00		7,500.00	
Total budget under the option	**14,026,408.75**	**115**	**15,048,380.00**	**127**	**14,903,648.75**	**125**	**19,379,380.00**	**178**
Combined costs of Option 2 a) and 3[109]	**31,690,557.75**	**136**	**33,085,389.00**	**153**	**32,567,797.75**	**146**	**37,416,389.00**	**204**
Combined costs of Option 2 b) and 3[110]	**28,406,722.75**	**138**	**29,897,797.00**	**156**	**29,283,962.75**	**148**	**34,228,797.00**	**207**
Combined costs of Option 2 c) and 3[111]	**28,190,557.75**	**136**	**29,585,389.00**	**153**	**29,067,797.75**	**146**	**33,916,389.00**	**204**

This second table provides more detailed information on the costs of the options. It presents the specific assumptions taken into account to calculate the costs of the factors for change. Please note that where synergies are expected (as detailed in the assumption column) the estimated costs are only taken into account once. Therefore, the costs indicated in the last column of this table cannot be added up to reach the total costs.

Table 28: Cost estimations for the options – detailed including assumptions

Options	Factors of change	Assumptions	Estimated costs/year
Option 0: Baseline, maintain the status quo: This option concerns an extension of the current mandate in terms of scope and objectives, though the provisions from the NIS Directive, the eIDAS Regulation and Telecoms Framework Directive would need to be taken into account.			
Revise ENISA's mandate to make its new tasks as per recent/upcoming	• **Involvement in Cooperation Group:** Support MS cooperation on drafting and maintaining over time voluntary guidelines on security measures for Operators of Essential	• It is assumed that ENISA will be able to take on all new tasks assigned to it as per recent legislative changes by reallocating responsibilities and tasks, as it has been done in the 2016 and 2017 Work	Human resource costs: Status quo to EUR 676,416

[109] Taking into account that the costs for a liaison office in Brussels would only have to be added once.

[110] Taking into account that the costs for a liaison office in Brussels would only have to be added once.

[111] Taking into account that the costs for a liaison office in Brussels would only have to be added once.

Options	Factors of change	Assumptions	Estimated costs/year
legislation more specific	Services, Incident Reporting, Identification of Essential Operators and Essential Service	Programme.	
	• **CSIRT Network Secretariat**: Provide technical support for back-end services that enable CSIRTs to exchange information on best practices and actual incidents and threats, as well as support voluntary cooperation in case of incidents	• Should this not be possible, ENISA could get another eight staff members (two for each of the key sectors finance, health, transport and energy) to respond to its new responsibilities. This represents eight FTEs at senior expert/analyst level (AD 7 to 12 grade).	
	• **Electronic communications code, recital 92**: Contribute to an enhanced level of security of electronic communications by, amongst other things, providing expertise and advice, and promoting the exchange of best practices		
	• **eIDAS**: (1) Recital 39 - Enable the EC and MSs to assess the effectiveness of the breach notification mechanism introduced by this Regulation by, for example, aggregating the national reports provided by supervisory bodies into an annual Report on EU Breaches in Trust Service Providers. (2) Support supervisory authorities in the drafting and supervision of security measures of Trust Services through, for example, supporting national regulators in the drafting and maintenance of guidelines on security measures and incident notification formats and procedures on Trust Services		
TOTAL COST OF OPTION 0		Assuming that all factors of change are being implemented	Current budget: EUR 11,244,679 Additional human resources costs: EUR 0 to EUR 676,416 Other additional costs: EUR 0 TOTAL: EUR 11,244,679 to 11,921,095

Options	Factors of change	Assumptions	Estimated costs/year
Option 1: Expiry of ENISA's mandate (terminating ENISA): This option would involve closing ENISA and not creating another EU-level institution, but relying on existing institutions/organisations to implement engagements under, for example, the NIS Directive and bilateral or regional ties at Member State level.			
N/A	N/A	N/A	Cost savings: The direct costs for the EU budget of not extending the mandate of ENISA in 2020 would be EUR 0, which implies thus a cost saving for the European institutions[112] of approximately EUR 10,332,000[113] yearly, plus a 2% standard increase per year. *Note that abstraction is made of any possible cost of e.g. re-allocating staff and the removal of infrastructure and all miscellaneous administrative requirements for ending ENISA's activities.*
Option 2: Enhanced ENISA (Keep ENISA with changes to its mandate): This option concerns making significant revisions to ENISA's mandate to address the key issues identified in the study, thereby building on its current role and ensuring that the new mandate is better adapted to the evolving cybersecurity landscape.			
Strengthen ENISA's operational role	• **Provide periodic threat intelligence and ad hoc alerts**: ENISA would develop and maintain its own threat intelligence capacity in order to monitor the threat landscape and provide MSs fast alerts/warnings on emerging threats and risks and monitor security incidents, including those affecting specific MSs. This would involve: (1) producing regular threat intelligence reports including high-level strategic analyses on threats, incidents and trends (e.g. key technological developments) and (2) collecting and analysing public communications on an event and compiling EU-level flash reports and guidance to	• Would need analysis capability and need to source the information which would require a kind of security operation centre (SOC) receiving feed or threat data which could come through individual CSIRTs. Would have automated tools to interpret what that data is saying and then a team of analysts to transpose what the tools are saying into something that makes sense. • ENISA have the staff necessary to conduct the preparatory analysis, but do not have anyone to conduct the technical, short-term, quick analysis • For the periodic threat intelligence: 6 to 8 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to engage and interpret the data and provide high level situational reports and a mix of	Human resource costs: EUR 531,000 to EUR 700,104 / year

---

[112] The financing provided by the Government of the Hellenic Republic (which constitutes between 6 and 7% each year), as well as contributions from third countries participating in the work of the Agency (around 1%) has been deducted from this estimate.

[113] Share of ENISA's budget in 2017 representing a subsidy from the EU budget.

Options	Factors of change	Assumptions	Estimated costs/year
	businesses and citizens.	IT players that understand the tools, senior subject experts/analysts (AD 7 to 12 grade) to interpret the data and with a multi-stakeholder experience (i.e. relations and links to industry, CSIRTs, EC3 etc.) • <u>For the ad hoc alerts</u>: 0.5 FTEs among the 6 to 8 FTEs (TAs) senior subject experts/analysts (AD 7 to 12 grade) above to focus on this and be able to scale when an incident takes place as will be on demand • *Note: An additional cost that could be incurred is derived from ENISA acquiring feed or threat data for a fee, but here it has been assumed that data would be channelled to it by CSIRTs*	
	• **Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level**: ENISA would: (1) organise cybersecurity exercises to test the Blueprint at all levels – operational, tactical and strategic) with all stakeholders; (2) collect and aggregate reports from national sources (CSIRTs) to establish a common situation awareness report for decision makers in the event of an incident; (3) support technical handling of the incident, including facilitating sharing of technical solutions between MSs; (4) handle public communication around the incident; (5) in case of a major crisis, propose the activation of the political decision making (IPCR) by alerting all or one of the EU institutions; (6) publish flash report or alerts in the event of significant events or incidents based on publically available information OR information made available through the CSIRT Network	• Would go hand in hand with the "Provide periodic threat intelligence and ad hoc alerts" change above for points 2 and 6 in particular, so synergies in the team could be exploited if both changes are implemented • Synergies could be exploited here with the communications team should this change be implemented • The organisation of cyber exercises would be scaled up by 50%: Would look at incident from beginning to end, involve a variety of stakeholders and would be carried out yearly (rather than every 2 years) • 6 to 8 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to engage and interpret the data and provide high level situational reports, as well as bridging the operational and strategic levels, being responsible for escalation and facilitation in a crisis situation; a communications professional with an understanding of cybersecurity to manage the press and support the Head of Unit; and a mix of IT players that understand the tools, senior subject experts/analysts (AD 7 to 12 grade) to interpret the data and with a multi-stakeholder experience (i.e. relations and links to industry, CSIRTs, EC3 etc.) • 0.5 FTEs among the 6 to 8 FTEs (TAs) senior subject experts/analysts (AD 7 to 12 grade) above	<u>Human resource costs</u>: EUR 531,000 to EUR 700,104 / year <u>Organisation of exercise costs</u>[114]: EUR 926,142 / year

---

[114] Based on the cost of the 2016 exercise which amounted to EUR 617,428.See ENISA Annual Activity Report 2015. https://www.enisa.europa.eu/publications/corporate/enisa-annual-activity-report-2015

Options	Factors of change	Assumptions	Estimated costs/year
		• to be able to scale up and support the technical handling of an incident when an incident takes place as will be on demand • *Note: An additional cost that could be considered and for which external funding could be sought is the updating of the platform used for these exercises – here it has been assumed that the existing platform will be employed*	
	• **Provide emergency cybersecurity response**: ENISA would provide on-demand technical assistance to MS bodies and institutions by creating and maintaining a team of experienced senior cybersecurity incident advisors who may be sent to MSs upon their request to assist and contribute to cybersecurity incident response and recovery	• Would be on-demand, so difficult to estimate the exact need, but synergies in the team "supporting the Blueprint for response to large scale cybersecurity incidents and crises at EU level" and the before and after incident response capability to be developed as part of this could be exploited • 15% of 4 FTEs (TAs) among the 6 to 8 FTEs (TAs) senior subject experts/analysts (AD 7 to 12 grade) above working on "Providing periodic threat intelligence and ad hoc alerts" and "Supporting the Blueprint for response to large scale cybersecurity incidents and crises at EU level" with experience in dealing with events in real time and advising, as well as contacts in the CERTs who could be called upon in the event of an incident	<u>Human resource costs</u>: EUR 50,731 / year
Strengthen ENISA's role in policy development and implementation	• Establish ENISA as an agency that has to be involved by other EU bodies, including the Commission, when cybersecurity matters are being considered • Formally involve ENISA in the implementation of the Connecting Europe Facility on Telecoms as an advisory body • Establish semi-formal governance structures with regular meetings between ENISA and other agencies/international organisations (e.g. on given common themes such as training) to increase cooperation at EU institutional level	• Would involve ENISA taking a more proactive approach where it would actively follow policy and play the role of a strong coordination body in this respect • Ideally, would need to have 2 FTEs per sector (i.e. energy, transport (aviation/vehicles), health, finance) to avoid a single point of failure • 9 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior sector-specific experts/analysts (AD 7 to 12 grade) • Estimated 15 meetings per month with travel and per diems for 1.5 staff/meeting on average – (where other than Brussels-based staff)	<u>Human resource costs</u>: EUR 784,656 / year <u>Meeting costs</u>[115]: EUR 175, 320 / year
	• Set-up a liaison office in Brussels with two to three permanent employees	• 2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to talk to MEPs, senior officials and go to meetings at short notice and senior experts/analysts (AD 7 to 12 grade) to follow through and execute what has been decided • Office space rental in Brussels at a cost of EUR 300	<u>Human resource costs</u>: EUR 243,125.75 to 349,753 EUR / year <u>Office space rental</u>: EUR 7,500 / year

Options	Factors of change	Assumptions	Estimated costs/year
		/square meter[116] and a need for an estimated office space of 25 square meters for 2 to 3 people	
	• Create a dedicated communications team within ENISA	• 2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) with experience in communications at different levels and understanding of cyber security and junior communications experts/analysts (AD 5 to 6 grade) to assist the Head of Unit	Human resource costs: EUR 112,454 to 116,668 / year
Make ENISA's mandate permanent	• This would involve ENISA having a permanent mandate, but still allow for the periodic evaluation of the performance of the Agency	• Would simply involve a revision of the mandate	N/A
Strengthen ENISA's governance structure	• Formally involve other stakeholders in the governance of ENISA by increasing the weight of the PSG in playing an advisory role on ENISA's Work Programme	• Would simply involve a revision of the mandate	N/A
	• Allow more flexibility for ENISA to determine its own work priorities at Executive Board level	• Would simply involve a revision of the mandate	N/A
Include a role for ENISA in EU-level standardisation and certification	• **Support the EU ICT Security Certification Framework**: Put in place an EU ICT security certification framework whereby ENISA would play a supporting role by (1) assisting the Commission in carrying out secretarial tasks and actively supporting the work undertaken (e.g. convene meetings of the framework's governance structures and meetings and engagements with industry stakeholders);(2) providing technical expertise to Member States (e.g. MS taking part in the framework on issues related to security testing and vulnerabilities in ICT products); and (3) compiling and publishing guidelines concerning the security requirements of ICT products and services in cooperation with national authorities and industry, thereby communicating the work of the framework to industry, consumers at Eu and international level	• Synergies could be exploited here with the team set-up to strengthen ENISA's role in policy development and implementation should this change be implemented • 4 to 6 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) including a mix of sector-specific experts and experts in certification (preferably with experience of industry or a good understanding of it), as well as multi-stakeholder expertise and an understanding of policy • Estimated 3 to 5 meetings/events per month with travel and per diems for 1.5 staff/meeting on average – (where other than Brussels-based staff)	Human resource costs: EUR 361,896 to 531,000 EUR / year Attendance at event/ meeting costs[117]: EUR 28,002 to 58,440 / year
	• **Support ICT security standardisation**:	• Would go hand in hand with the "Support the EU	Human resource costs:

---

[116] Source: Rental prices of prime office properties in selected European cities as of 4th quarter 2016 (in euros per square meter per year). The Statistics Portal. https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/

[117] Return trip estimated at EUR 500 and per diems at EUR 224 on the basis of an average of EuropeAid per diem rates for Europe – see https://ec.europa.eu/europeaid/sites/devco/files/perdiems-2017-03-17_en.pdf

Options	Factors of change	Assumptions	Estimated costs/year
	ENISA would provide a supportive role in facilitating the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services, including by cooperating with Member States on technical areas concerning the security requirements for operators of essential services and digital service providers. This could involve supporting the work of the EU ICT Security Certification Framework in EU and international standard organisations; taking part in and contributing to the work of cybersecurity working groups of the European Standardisation Organisations (ESCs); performing reviews and assessments of cybersecurity related standards when associated with regulatory and legal requirements (e.g. eIDAS)	ICT Security Certification Framework" change above as the issues are related and there would be a need to avoid silos, so synergies in the team could be exploited if both changes are implemented in order to avoid single points of failure • 4 to 6 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) including a mix of sector-specific experts and experts in standardisation/certification (preferably with experience of industry or a good understanding of it), as well as multi-stakeholder expertise and an understanding of policy • 0.5 FTEs among the 4 to 6 FTEs (TAs) above to be used for the stock taking, compiling and reviewing of standards	EUR 361,896 to 531,000 EUR / year
Strengthen ENISA's position relative to research and innovation	• **Take part in programming implementation**: ENISA would implement parts of the Framework Programme for R&I which relates to cybersecurity whereby the EC delegates the relevant powers by performing the following tasks: (1) managing some stages of then programme implementation and some phases in the lifetime of specific projects on the basis of WPs adopted by the EC; (2) adopting the instruments of budget execution for revenue and expenditure and carrying out all the operations necessary for the management of the programme; and (3) providing support in programme implementation. Examples of the activities ENISA could perform include implementing calls on Public Procurement of Innovation (PPI) in close collaboration with MS authorities, and support MS public procurers in identifying common research and innovation requirements.	• ENISA would perform a similar function with respect to R&I to that foreseen as part of the new Frontex Regulation[118]	<u>Estimated costs based on similar function foreseen for Frontex</u>: EUR 3.5m / year

---

[118] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC, COM(2015) 671 final. See SPECIFIC OBJECTIVE NO 6 "Management of Pooled resources and R&D. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation_on_the_european_border_and_coast_guard_en.pdf

Options	Factors of change	Assumptions	Estimated costs/year
	• **Take part in programming through playing an advisory role:** ENISA would play an expert advisory role in the cyber security-related elements of EU R&D funding programmes (H2020, CEF) by sitting on an advisory committee, providing independent advice and input and feeding into ideas for research.	• Synergies could be exploited here with the team set-up to strengthen ENISA's role in policy development and implementation should this change be implemented • Advisors would need to draw on the knowledge of sector experts/analysts for input • 2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) • Estimated 2 to 3 meetings per month with travel and per diems for 1.5 staff/meeting on average – (where other than Brussels-based staff)	Human resource costs: EUR 192,792 to 277,344 EUR / year Meeting costs: EUR 23,373 to 35,064 /year
	• **Benefit from EU R&I funding**: Open ENISA's mandate to take part in EU R&D funding programmes (H2020, CEF) as a recipient of funding by changing the provisions on source of revenue but not adding it as a task. ENISA can provide added value to industry and academia in R&I by leveraging its practical expertise in areas such as cooperation, information sharing and regulatory requirements.	• Would simply involve a revision of the mandate	N/A
TOTAL COST OF OPTION 2		Assuming that all factors of change are being implemented There are different factors of change to strengthen ENISA's position relative to research and innovation which exclude one another due to issues of conflict of interest. Sub-option a) represents the costs for the factor of change under which ENISA will take part in programme implementation of the Framework Programme for R&I. Sub-option b) includes the costs of ENISA taking part in programming through playing an advisory role in EU R&D funding. Sub-option c) includes the costs of ENISA befitting from EU R&I funding (which are nil).	Current budget: EUR 11,244,679 Additional human resources costs: a) EUR 2,033,131.75 to EUR 2,482,181 b) EUR 2,225,923.75 to EUR 2,759,525 c) EUR 2,033,131.75 to EUR 2,482,181 Other additional costs: a) EUR 4,636,964 to EUR 4,667,402 b) EUR 1,160,337 to EUR 1,202,466 c) EUR 1,136,964 to EUR 1,167,402 TOTAL: a) EUR 17,914,774.75 to EUR

Options	Factors of change	Assumptions	Estimated costs/year
			18,394,262 b) EUR 14,630,939.75 to EUR 15,206,670 c) EUR 14,414,774.75 to EUR 14,894,262
Option 3: European Agency with full operational capabilities (establish a European Centre of Cybersecurity): This option concerns developing ENISA into a new body at EU level that would cover the entire cycle cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.			
Create an EU level cyber security umbrella	• Develop an umbrella organisation covering ENISA and CERT-EU, thereby bringing together three main functions, namely policy advice, centre for information and Computer Emergency Response Team. The operational role of CERT-EU in responding to cyber incidents in the EU institutions would therefore be combined with ENISA's role of ensuring cooperation in the event of an incident. The new organisation would act as an EU contact point for cybersecurity related issues in close coordination with the EEAS. • Options include merging ENISA and CERT-EU and having a governance structure that would allow different reporting lines and oversight for the team dealing with the EU institutions, or integrating CERT-EU within ENISA as one of the Agency's departments.	• If this option is adopted, ENISA would be in the position to "Provide periodic threat intelligence and ad hoc alerts" and "Support the Blueprint for response to large scale cybersecurity incidents and crises at EU level" (see above – Option 2) by using a combination of ENISA and CERT EU staff. • Most of the changes referred to above in relation to "Providing periodic threat intelligence and ad hoc alerts" and "Supporting the Blueprint for response to large scale cybersecurity incidents and crises at EU level" (see above – Option 2) would come for free (i.e. anything related to response side, e.g. flash notes, following up on incidents etc.) as CERT-EU have the capacity internally to deal with this • Relocation of ENISA to Brussels would not be necessary, but the establishment of a liaison office would Costs linked to the establishment of a liaison office (as above): • Synergies could be exploited here with the team set-up to strengthen ENISA's role in policy development and implementation should this change be implemented • 2 to 3 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) to talk to MEPs, senior officials and go to meetings at short notice and senior experts/analysts (AD 7 to 12 grade) to follow through and execute what has been decided • Office space rental in Brussels at a cost of EUR 300 /square meter[119] and a need for an estimated office space of 25 square meters for 2 to 3 people	Human resource costs: EUR 243,125.75 to 349.753 EUR / year Office space rental: EUR 7,500 / year Efficiency gains: This option would involve combining or ENISA absorbing the current staff of CERT EU. There is the potential to create synergies and decrease costs through the ability to spread tasks over 2 teams with complementary skill-sets.

---

[119] Source: Rental prices of prime office properties in selected European cities as of 4th quarter 2016 (in euros per square meter per year). The Statistics Portal.
https://www.statista.com/statistics/431672/commercial-property-prime-rents-europe/

Options	Factors of change	Assumptions	Estimated costs/year
		• *Note: Change management costs would be incurred but it is outside of the scope of this study to assess these*	
Create a virtual European CSIRT	• **Coordinate CSIRT Network operations**: Enable the Agency to coordinate the operations of MS CSIRTs, collecting information and pooling national resources on analysing threats and responding to incidents	• ENISA would act as a facilitator as the expertise would come from the Member States themselves • Could second people to/draft people in from Member State CSIRTs to build a virtual European CSIRT and then have an aggregation of information so what is sensitive to Member States is taken out without losing the contextual picture • 4 to 5 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) to put the infrastructure in place, and carry out the outreach with industry in Member States, through the ISACs at sectoral, with CSIRTs etc.	Human resource costs: EUR 361,896 to EUR 446,448 EUR / year
	• **Produce real time situational awareness and dynamic (live) threat intelligence feeds**: Enable ENISA to act as a broker, sharing information on incidents between Member States in the form of real-time situational awareness and dynamic (live) threat intelligence feeds on the basis of information exchanged on the CSIRT Network	• Would be an observatory in real time • First there will be a need to set-up the necessary infrastructure, including the communication links across Europe with a variety of players (industry, ISACs). This would result in the establishment of a security operation centre (SOC) that would process and share the data, report to the press and conduct briefings at political level. • <u>Initial set-up</u>: 10 to 15 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) to put the infrastructure in place. • <u>Once up and running</u>: 5 to 6 FTEs (TAs) - including 1 Head of Unit (AD9 to AD14 grade) to engage at the right levels and across sectors, and senior (ICT) experts/analysts (AD 7 to 12 grade) to process and analyse the data real time through a roster (24/7) and in order to avoid single points of failure	Human resource costs: *(1) Initial set-up*: EUR 869,208 to 1.3m / year *(2) Once up and running*: EUR 446,448 to 531,000 EUR / year
	• **Maintain and provide own cybersecurity incident response capacity to public and private sector**: ENISA would create and maintain the capacity to provide on-demand technical operational assistance to MS CSIRTs, operators of essential services, EU	• The scope and scale of this task could vary extensively depending on the breadth of "clients" of the service, e.g. whether SMEs or not etc. • <u>Initial set-up</u>: 15 to 20 FTEs (TAs) – including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade) to put the	Human resource costs: *(1) Initial set-up*: EUR 1.3m to 1.7m / year *(2) Once up and running*:

Options	Factors of change	Assumptions	Estimated costs/year
	bodies and institutions for the prevention, detection and response to incidents	infrastructure in place. • <u>Once up and running</u>: 30 to 80 FTEs[120] (TAs) - including 1 Head of Unit (AD9 to AD14 grade) and senior experts/analysts (AD 7 to 12 grade)	EUR 2.6m to 6.8m / year *Note as a means of comparison (and while keeping in mind the differing aims of these centres) that Frontex runs a 24/7 situation centre at an average cost of EUR 3.0m / year, as per the new Frontex Regulation[121]*
TOTAL COST OF OPTION 3		Assuming that all factors of change are being implemented	Current budget: EUR 11,244,679 YEAR 1 Additional human resources costs: EUR 2,774,229,75 to EUR 3,796,201 Other additional costs: EUR 7,500 TOTAL: EUR 14,026,408.75 to EUR 15,048,380 YEAR 2-5 Additional human resources costs: EUR 3,651,469.75 to EUR 8,127,201 Other additional costs: EUR 7,500 TOTAL: EUR 14,903,648.75 to EUR 19,379,380
TOTAL COST OF OPTION 2 AND OPTION 3 COMBINED		Assuming that all factors of change are being implemented Taking into account that the costs for a liaison office in Brussels would only have to be added once	YEAR 1 Option 2a and 3: EUR 31,690,557.75 to EUR 33,085,389 Option 2b and 3: EUR 28,406,722.75 to EUR 29,897,797 Option 2c and 3: EUR 28,190,557.75 to EUR

---

[120] Based on an average of the number of FTEs employed in CERT-EU (30 FTEs) and in the larger Member State CERTs

[121] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Border and Coast Guard and repealing Regulation (EC) No 2007/2004, Regulation (EC) No 863/2007 and Council Decision 2005/267/EC, COM(2015) 671 final. See SPECIFIC OBJECTIVE NO 7 "EUROSUR and situational picture" https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/regulation_on_the_european_border_and_coast_guard_en.pdf

Options	Factors of change	Assumptions	Estimated costs/year
			29,585,389 YEAR 2-5 Option 2a and 3: EUR 32,567,797.75 to EUR 37,416,389 Option 2b and 3: EUR 29,283,962.75 to EUR 34,228,797 Option 2c and 3: EUR 29,067,797.75 to EUR 33,916,389

APPENDIX 1
EVALUATION QUESTION MATRIX

Table 29: Evaluation questions matrix

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
EFFECTIVENESS				
EQ1 To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate?	**Retrospective** EQ2: What have been the benefits of acting at Agency level both from the operational and strategic perspective? EQ3: To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe? What more could be done? EQ4: How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders? *EQ5: To what extent has ENISA become an EU-wide centre of expertise and a reference point for stakeholders[122] in providing guidance, advice and assistance on issues related to network and information security?[123] EQ6: How effectively has the Agency managed to set its work priorities? EQ7: How effectively does the Agency tackle important upcoming, unplanned issues deriving by demands of its constituencies and/or EU policy priorities?	Activity level indicators: Number of training courses, exercises, publications (e.g. training material, toolkits, BP guides, reports, roadmaps), methodologies, workshops, conferences. Output level indicators: - Number of responses to Article 14 requests 2013-2016 - Number of guidelines issued and disseminated 2013-2016 - Number of recommendations issued and disseminated 2013-2016 - Number and type of participants in trainings, workshops, exercises 2013-2016 - Number of downloads of different types of publications (e.g. training material, BP guides etc.) - Number and type of standards established Result level indicators: - Stakeholders' views on the extent to which ENISA has achieved its objectives as per its mandate. - Degree to which stakeholders' have made use of material, followed recommendations and guidelines, copied BPs - Degree to which stakeholders have disseminated material, guidelines, BPs more widely -Overall degree of achievements of objectives – as per specific M&E framework (yearly adapted to core	Products (e.g. publications/papers) and services are delivered as planned. The activities carried out by the Agencies are shown to support the achievement of the objectives. 70% of objectives and intended results were reached and where objectives or results were not reached this is accounted for (cross-checking KPIs and stakeholder´s assessments). Users are satisfied with the products and services (no issue is mentioned)[127] Mechanisms are in place to ensure that the	Data sources: Desk research – annual reports, in particular reporting on the KIIs[128] Results of ENISA's follow-up activities relating to exercises, trainings, workshops, events Results of the evaluations of ENISA's activities of 2014 and 2015 In-depth interviews Public consultation (excluding EQ11)

---

[122] The stakeholders include EU institutions, Members States and the wider stakeholders community

[123] This question has been reformulated to ensure that it is open. The original question was: "To what extent ENISA became an EU-wide centre of expertise and a reference point for EU institutions, Members States and the wider stakeholders community, in providing guidance, advice and assistance on issues related to network and information security?"

[127] This judgement criterion is also expected to rely on the assessments made in relation to evaluation question related to the evaluation criterion relevance.

[128] Please note that, as concluded in the evaluation of ENISA's 2015 core operational activities, while some KIIs are situated at the impact level and data has been collected in relation to them, it was found that it was too early to report on many of the indicators. An additional challenge is that the KIIs change on an annual basis, making it difficult to monitor results on a year-on-year basis as there is no requirement to do so. Some of the indicators are situated at the output/result levels and will be used to report in relation to the indicators set out in this matrix.

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	EQ8: Does the Agency consistently perform the same tasks with the same quality level over time? EQ9: How does ENISA compare to the other EU and national bodies offering similar services in relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency? *EQ11: How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to effectiveness in the work of the agency?[124] EQ12: How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate? EQ13: What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives? *EQ19: To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc.)?[125] *EQ20: To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?[126]	operational activities) Impact level indicators: - Stakeholders' perceptions on the extent to which ENISA contributed to the overall EU goal of increasing network and information security in Europe, and what more could be done. Degree to which there are internal/external factors to ENISA which influence / restrict progress Other indicators: Mapping of the Agencies' structured quality management processes (gathering and analysing feedback from users). Mapping the process of developing multi-annual work programmes. Evidence of adjustments to annual work programmes, justified by policy, political or economic changes. Stakeholders' assessment of the Agencies' ability to adapt to policy, political or economic changes. Expert assessment of whether evaluation/monitoring requirements and practices are adequate compared to the Better Regulation Guidelines. A comparison of make or buy between similar agencies, e.g. procurement/operational budget. Mapping of how make or buy (or a hybrid form) decisions have been made.	products (e.g. publications/papers) and services developed continuously meet the needs of the users. It can be documented that ENISA's products and services are used by a wide range of national and European stakeholders.	Survey of ENISA staff (only for EQ11)

---

[124] This question has been reformulated by removing a reference to "efficiency", which will be covered by EQ14 and its sub-questions. The original question was: "How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to efficiencies and effectiveness in the work of the agency?".

[125] This question was originally (in the Roadmap) included under efficiency, but is better suited under effectiveness.

[126] This question was originally (in the Roadmap) included under efficiency, but is better suited under effectiveness.

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	Prospective *EQ37: How does the new policy and regulatory landscape, having regard for the recently adopted Network and Information Security Directive and COM(2016) 410, and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?[129] *EQ38: What are the main strengths and weaknesses of ENISA in taking up new challenges, considering its current mandate and organisational set-up and capacity?[130] *EQ39: If ENISA should take on any new challenges and tasks, would a fixed-term mandate be suitable?[131] EQ41: Which are the concrete needs and opportunities for cooperation and synergies with international bodies working in adjacent fields, like the NATO Cooperative Cyber Defence Centre of Excellence?	Findings from the research done for EQ1-9, EQ11-13, EQ19 and EQ20. Stakeholders' assessment of the Agency's mandate main strength(s) and weakness(es) in view of taking up new challenges. Stakeholders' assessment of the Agency's organisational set-up and capacity main strength(s) and weakness(es) in view of taking up new challenges. Stakeholders' assessment of the optimal type of mandate. Expert assessment of the optimal type of mandate.	*Since the prospective EQs are explorative it is not recommendable to define judgement criteria (as there is no justified basis).*	Data sources: Public consultation and in-depth interviews
EFFECIENCY				
EQ14: To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation? To assess this	**Retrospective** *EQ15: Were the annual budgets of the Agency implemented in an efficient way considering the results achieved?[132] EQ16: Have the resources allocated to the Agency been sufficient for the pursuit of its tasks (input/output analysis)?	Tracking of cost/resources used per deliverable Cost per download for reports Cost saving measures are in place % of staff positions filled (on an annual basis) % of staff members working on core operations.	Stable costs, and decreases/increases can be justified Continuous work/processes in place to save costs in the operations	Data sources: AARs, Governing Boards analysis and assessment of the AARs, in-depth interviews

---

[129] This question has been revised based on comments from the Commission. It was originally (in the Roadmap) "How does the new policy and regulatory landscape, having regard to the recently adopted Network and Information Security Directive, in COM(2016) 410 , and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?"

[130] This question has been re-worded to improve clarity. The original question was: "What are the main strengths and weaknesses of ENISA, within its current mandate and organisational set-up and capacity, in taking up new challenges?"

[131] This question has been re-worded to improve clarity. The original question was: "Is a fixed-term mandate coherent with the new challenges and tasks ENISA will have to take on?"

[132] This question has been re-worded to improve clarity. The original question was "Were the annual budgets of the Agency implemented in an efficient way with a view on achieved results?"

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
question, elements relating to internal structure, operation, programming of activities and resources, accountability and controls, etc. will be analysed.	*EQ17: To what extent are the organisational solutions and procedures of ENISA adapted to the work entrusted to it and to the actual workload?[133] Is the planning cycle of the agency (work programme and budget) in line with the objective of achieving efficient results? EQ18: To what extent have ENISA's governance, organisational structure, locations and operations as set in its Regulation and the arrangements related to the location of its offices been conducive to efficiency and to achieving economies of scale? EQ21: To what extent and how have external factors influenced the efficiency of ENISA? *Please note that EQ19 and EQ20 were originally (in the Roadmap) included under efficiency, but have here been organised under effectiveness as this is more appropriate.	Agencies' managerial staff assessment of flexibility in adjusting staff composition Share of budget allocated to administrative tasks Existence of own implementation rules (approved by the Commission) Prevalence of use of external expertise % of publications and similar deliverables where dissemination/ communication was successful Number of studies procured vs. number of studies produced in-house", including relative to other comparable organisations Typologies of what triggers procurement decisions (need for expertise, resource constrains or other) , including relative to other comparable organisations Drivers and inhibitors in the budgeting process. Usage of permanent stakeholder groups/bureaus or similar[134] and use of advisory committees/working groups or similar. Development in location costs during the period (compared to a 2009 baseline). % of agency staff and management which assess that the Headquarters Agreement is fulfilled. Host member states assessment of the extent to which the Headquarters Agreement is fulfilled Positive/negative assessments from the respective Governing Boards of the AARs.	Follow-up measures in place Evidence of efficient management of the resources available with improvements in the balance between operational budgets and administrative budgets achieved where necessary (based on previous evaluations, audits or similar). Evidence can be provided on how current organisation allows for optimal use of capabilities and resources: •Division of work and resources are appropriate •Shared resources are available •Cooperation is encouraged facilitated No organisational obstacles are encountered in the delivery of products and services The internal organisational structure for the delivery of products and services allow for the most	

---

[133] This question has been re-worded to improve clarity. The original question was "To what extent are the organisational solutions and procedures of ENISA adequate to the work entrusted to it and to the actual workload?"

[134] Several EU decentralised Agencies have established such groups in order to consult/engage/involve stakeholders in the Agencies work, for example annual work programme's priorities.

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
			optimal use of capabilities and resources: •no gap is identified •no redundancy is found	
	Prospective *EQ42: Could ENISA's mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape or would another EU initiative be more efficient?[135] EQ43: What would be the financial implications associated with each of the possible options for modifying ENISA's mandate as they emerge from the evaluation?	Findings from EQ14-18, and EQ21 as well as EQ 36.	*Since the prospective EQs are explorative it is not recommendable to define judgement criteria (as there is no justified basis).*	Data sources: Public consultation (only for EQ42)
RELEVANCE				
EQ33: Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework and needs?	**Retrospective** EQ29: How far are the Agency's tasks and resources aligned with key EU political priorities? EQ30: Which Agency tasks are absolutely essential to deliver on these priorities? EQ31: Which Agency tasks are necessary to continue implementing existing and evolving obligations under the Treaties and EU legislative framework? EQ32: Are there some Agency tasks that have become redundant / negative priorities? If so, which are they? EQ34: Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?	Mapping of structured quality management processes (gathering and analysing feedback from users). % of KPIs related to uptake of the Agencies expertise in policy documents or by industry. % of KPIs related to the Agencies contribution to policy development through events. Users' assessment of the extent to which the agency fulfils current needs. Estimate of media-coverage of the Agency (which reaches a broader audience) New stakeholders are engaged when appropriate (e.g. new sign-ups for newsletters, new consultations or similar).	Mechanisms are in place to ensure that the products and services developed continuously meet the needs of the users. All existing products and services provided by the Agencies' correspond to current needs (no issues are mentioned) All current needs are fulfilled (no gaps are identified)	Data sources: Public Consultation, in-depth interviews, staff survey (only for EQ34)
	Prospective	Findings from EQ29-EQ34.	*Since the prospective EQs are explorative it is*	Data sources: Public

---

[135] This question has been revised based on comments from the Commission to the inception report. The origanl question (from the Roadmap) was: "How could ENISA's mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape?"

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	*EQ36: Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent is ENISA best placed to respond to these needs? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?[136] EQ40: Which are the concrete needs and opportunities for further increased practical cooperation with Member States and EU bodies?	Stakeholders assessment of needs which are not addressed, weighed against the relevance of ENISA providing them.	*not recommendable to define judgement criteria (as there is no justified basis).*	consultation
COHERENCE				
*EQ24: To what extent are ENISA activities coherent with the policies, strategy documents and activities of other stakeholders?[137]	**Retrospective** EQ22: To what extent is ENISA acting in cooperation with *the European Commission and other EU bodies*, to ensure complementarity and avoid duplication of efforts? EQ23: To what extent is ENISA acting in cooperation with the *Member States* to ensure complementarity and avoid duplication of efforts? EQ25: Are the procedures put in place effective to ensure that ENISA's cooperation activities are coherent with the policies and activities of its stakeholders? EQ26: What are the risks/sources of overlaps/conflict of interests?	Comparison of the ENISA's mandate, objectives and activities to comparable organisations/bodies, including potential overlap between stakeholders/users Number of joint workshops and deliverables between ENISA and cooperation partners. Identification of areas in which ENISA cooperates closely with other EU, national or international bodies. Mapping of coordination mechanisms in place between the Agencies. Stakeholders' assessment of whether there is coherence between ENISA and other policies and activities of its stakeholders.	The mandates, objectives and activities of the ENISA are: • complementary to the work carried out by national/European/ international stakeholders (do not duplicate) Sources of complementarity and synergy are systematically utilised	Data sources: Public Consultation, in-depth interviews
	Prospective *EQ45: Taking into account the new tasks (identified during the evaluation), will there be any risk of ENISA's tasks and activities overlapping with those of other national, European or international bodies working?	Findings from EQ22-26, and EQ29-34, and EQ36	*Since the prospective EQs are explorative it is not recommendable to define judgement criteria (as there is no justified basis).*	Data sources: Interviews and Public consultation

---

[136] This question has been reformulated based on comments from the Commission. The original question was: "Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent could ENISA's current mandate, tasks and/or capabilities address these needs?" Please note that the evaluator considers this question key in assessing upcoming and future needs.

[137] This question has been reformulated for clarity and comprehensiveness. The original question was: "To what extent are ENISA activities coherent with the strategy documents adopted in this policy field?"

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	Please note that findings related to EQ29-34 will also be relevant to answer this question (EQ41).			
EU ADDED VALUE				
EQ27: What would be the most likely consequences at the EU level of stopping ENISA?	**Retrospective** *EQ10: To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements?[138]EQ45: What has been the added value of having an EU cybersecurity agency such as ENISA over the period 2013-2016?[139]	Extent to which stakeholders' assess that the Agency has strengthened existing EU or national initiatives (volume effects) Extent to which stakeholders' assess that the Agency has carried out new initiatives (initiatives not part of existing EU or national initiatives, such as new areas of research or training) (scope effects) Share of stakeholders/Member States which consider that actions could not have been carried out without the support of the Agencies (including examples of innovative actions) (potential scope or role effect). Share of stakeholders/Member States which report additional benefits derived from the products or services (comparison with baselines from previous evaluations where possible) (potential role or process effects). Comparison of the Agencies ability to deliver results (derived from EQ1 above) to the upcoming multi-annual programmes. Stakeholders assessment of other similar organisations ability to deliver the needed results.	EU added value is identified and acknowledged	Data sources: Desk research, in-depth interview
	Prospective EQ28: How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place? EQ35: What would be the most likely consequences at the EU level of stopping ENISA's activities?	Cross-checking of whether the new challenges and tasks fit within the EU added value identified or not identified in the findings for EQ10, EQ27-28, and EQ35.	*Since the prospective EQs are explorative it is not recommendable to define judgement criteria (as there is no justified basis).*	Data sources: Interviews and Public consultation

---

[138] This question has been added by the evaluator.

[139] This question has been added by the evaluator based on comments received from the Commission to the Interim Report. It was not presented in the Roadmap for the evaluation of ENISA.

Evaluation Question	Sub-questions	Indicators	Judgement criteria	Data sources
	*EQ44: If any new tasks for ENISA are identified (e.g. through EQ4 and EQ37), do these represent EU added value?[140]			

---

[140] This question has been added by the evaluator.

APPENDIX 2
BIBLIOGRAPHY

1.   LEGAL SOURCES

Directive 2009/136/EC of the European Parliament and of the Council, of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws

Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation(EC) No 460/2004

Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2.   POLICY DOCUMENTS

Commission Staff Working Document. Executive Summary of the Impact Assessment accompanying the document 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union'; SWD (2013) 31 final

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for A European Policy Approach; COM/2001/0298 final

Communication from the Commission: Europe 2020: A strategy for smart, sustainable and inclusive growth; COM (2010) 2020 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions regarding 'A Digital Single Market Strategy for Europe'; COM (2015) 192 final

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry; COM (2016) 410 final

Council of the European Union (2014): Information note - Recommendations by the inter-institutional Steering Board of the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU) on the future mandate, governance, organisational setup, staffing and funding of CERT-EU. Brussels, 9 September 2014 – document number 12992/14

Council of the European Union (2015): Information note - CERT-EU mandate, service catalogue and information sharing and exchange framework. 3 March 2015 – document number 6738/15

European Commission (2010): Commission working document – Impact assessment accompanying document to the Proposal for a Regulation of the European Parliament and the Council concerning the European Network and Information Security Agency (ENISA); SEC(2010) 1126

European Commission, DG CNECT – H1, Evaluation Roadmap for the Evaluation of the European Union Agency for Network and Information Security (ENISA), 25/07/2016. Available at: https://ec.europa.eu/info/law/law-making-process/better-regulation-why-and-how_en. Accessed 16 May 2017

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: An Open, Safe and Secure Cyberspace'; JOIN (2013) 1 final

Study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs: 'Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses'. Study for the LIBE Committee. September2015. Available at: www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf. Accessed 16 May 2017

3. ENISA'S PUBLICATIONS, PROGRAMMING AND REPORTING DOCUMENTS

ENISA (2013): National-level Risk Assessments – An analysis report. ISBN: 978-92-9204-073-4; DOI: 10.2824/2633.

ENISA (2014): Annual Report 2013; ISBN: 978-92-9204-08; DOI: 10.2824/31416

ENISA (2015): Annual Activity Report 2014; ISBN: 978-92-9204-124-3; DOI: 10.2824/521040.

ENISA (2015): CYBER 7: Seven messages to the edge of Cyber-Space; ISBN: 978-92-9204-133-5; DOI: 10.2824/850678.

ENISA (2015): Threat Landscape and Good Practice Guide for Software Defines Networks/ 5G; ISBN: 978-92-9204-161-8; DOI: 10.2824/67261.

ENISA (2016): Annual Activity Report 2015; ISBN: 978-92-9204-167-0; DOI: 10.2824/698162

ENISA (2016): ENISA Strategy 2016-2020; ISBN: 978-92-9204-170-0; DOI: 10.2824/17857.

ENISA (2016): Events - 5th ENISA/EC3 Workshop. Available at: https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop. Accessed 30 May 2017

ENISA (2017): Privacy and Security in Personal Data Clouds – Final Report. ISBN: 978-92-9204-182-3; DOI: 10.2824/24216

Ramboll, Euréval, Matrix insight (2009): Evaluation of the EU decentralized agencies in 2009, Final Report Volume III – Agency level findings. Available at: https://europa.eu/european-union/sites/europaeu/files/docs/body/agency_level_findings_en.pdf. Accessed 30 May 2017

Ramboll Management Consulting (2015) External Evaluation of ENISA, focussing on ENISA's 2014 activities.

Ramboll Management Consulting (2016) External Evaluation of ENISA, focussing on ENISA's 2015 activities.

4. ACADEMIC LITERATURE

Bendiek, A. (2012). 'European Cyber Security Policy', SWP Research Paper No13. Available at: www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html. Accessed 16 May 2017

Carrapico, H., and Barrinha, A. (2017). 'The EU as a Coherent (Cyber)Security Actor?', JCMS: Journal of Common Market Studies, DOI: 10.1111/jcms.12575. Available at: http://onlinelibrary.wiley.com/doi/10.1111/jcms.12575/epdf. Accessed 16 May 2017

Christou, G. (2014): The EU's Approach to Cyber Security. EUSC EU China Security Cooperation: performance and prospects. Policy paper series. Available at: http://privatewww.essex.ac.uk/~susyd/EUSC/documents/EUSC%20Cyber%20Security%20EU%20 Christou.pdf. Accessed 16 May 2017

Fahey, E. (2014): EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security. European Journal of Risk Regulation, Vol. 5, No. 1, pp. 46-60. Available at: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2384491_code1636539.pdf?abstractid=23844 91&mirid=1. Accessed 16 May 2017

5. NATIONAL AND EU CYBERSECURITY BODIES

Agencia Estatal Boletín Oficial del Estado (2017): Legislación – Código de Derecho de la Ciberseguridad. Available at: http://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Cibersegur idad. Accessed 30 May 2017

ANSSI (2016): ANSSI, ready for the 2016 European Cybersecurity Month (ESCM). Available at: https://www.ssi.gouv.fr/en/actualite/anssi-ready-for-the-2016-european-cybersecurity-month-escm/. Accessed 30 May 2017

ANSSI (2016) : Rapport d'activité 2015. Available at: https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf. Accessed 30 May 2017

ANSSI (2016): "Stronger together" – ANSSI successfully took part in pan-European Exercise Cyber Europe 16. Available at: https://www.ssi.gouv.fr/en/actualite/stronger-together-anssi-successfully-took-part-in-pan-european-exercice-cyber-europe-16/. Accessed 30 May 2017

ANSSI (2017): Administration – bonnes pratiques. Available at: https://www.ssi.gouv.fr/administration/bonnes-pratiques/. Accessed 30 May 2017.

ANSSI (2017): Crypto – Le webdoc'. Available at: https://www.ssi.gouv.fr/entreprise/actualite/crypto-le-webdoc/. Accessed 30 May 2017

ANSSI (2017): Entreprise – bonnes pratiques. Available at: https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/. Accessed 30 May 2017

ANSSI (2017): Entreprise – Certification. Available at: https://www.ssi.gouv.fr/entreprise/produits-certifies/. Accessed 30 May 2017

ANSSI (2017): Entreprise – principales menaces. Available at: https://www.ssi.gouv.fr/entreprise/principales-menaces/. Accessed 30 May 2017

ANSSI (2017): Particuliers – bonnes pratiques. Available at: https://www.ssi.gouv.fr/particulier/bonnes-pratiques/. Accessed 30 May 2017

Certsi (2017): Alerta Temprana – Avisos SCI. Available at: https://www.certsi.es/alerta-temprana/avisos-sci. Accessed 30 May 2017

Certsi (2017): Servicios operadores – Detector de incidentes. Available at: https://www.certsi.es/servicios-operadores/detector-de-incidentes. Accessed 30 May 2017

Certsi (2017): Servicios operadores – Notificaciones y análisis ad hoc. Available at: https://www.certsi.es/servicios-operadores/notificaciones-y-analisis-adhoc. Accessed 30 May 2017

CERT-EU (2011): RFC 2350. Available at: http://cert.europa.eu/static/RFC2350/RFC2350_CERT-EU_v1_0.pdf. Accessed 30 May 2017

CERT-EU (2016): About us. Available at: https://cert.europa.eu/cert/plainedition/en/cert_about.html. Accessed 30 May 2017

Cyber Camp (2017): Summer boot camp. Available at: https://cybercamp.es/summer-bootcamp. Accessed 30 May 2017

DG JRC (2012): Will the cloud make the citizen more vulnerable? Risk and vulnerability assessment in times of cloud computing. Available at: https://ec.europa.eu/jrc/en/publication/contributions-conferences/will-cloud-make-citizen-more-vulnerable-risk-and-vulnerability-assessment-times-cloud-computing. Accessed 30 May 2017

DG JRC (2015): Risk assessment methodologies for critical infrastructure protection. Available at: http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf. Accessed 30 May 2017

Europol (2017): European Cybercrime Centre – EC3. Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-2. Accessed 30 May 2017

Europol (2017): Training and capacity building. Available at: https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building. Accessed 30 May 2017

INCIBE (2015): Gestión de riesgos – Una guía de aproximación para el empresario. Available at: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf. Accessed 30 May 2017

INCIBE (2015): INCIBE presenta la plataforma de NIS, como herramienta de la Estrategia Europea de Ciberseguridad, en el Infoday Horizonte 2020. Available at: https://www.incibe.es/sala-prensa/notas-prensa/nw-infoday-raul-riesco. Accessed 30 May 2017

INCIBE (2015): Taxonomía de ciberejercicios. Available at : https://www.certsi.es/sites/default/files/contenidos/estudios/doc/incibe_taxonomia_ciberejercicios.pdf. Accessed 30 May 2017

INCIBE (2016): 10 Encuentro internacional de seguridad de la información. Available at: https://www.incibe.es/en/enise. Accessed 30 May 2017

INCIBE (2016): El Instituto Nacional de Ciberseguridad representa los intereses nacionales en el European Cyber Security Organisation (ECSO). Available at: https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-representa-los-intereses-nacionales-el. Accessed 30 May 2017

INCIBE (2017): Formación especializada. Available at: https://www.incibe.es/formacion. Accessed 30 May 2017

INCIBE (2017): Protege tu empresa – Guías. Available at: https://www.incibe.es/protege-tu-empresa/guias. Accessed 30 May 2017

INCIBE (2017): Welcome to INCIBE. Available at: https://www.incibe.es/en. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2012): Factsheet Beveilig apparaten gekoppeld aan internet. Available at: https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-apparaten-gekoppeld-aan-internet.html. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2015): Checklist beveiliging van ICS/SCADA systemen. Available at: https://www.ncsc.nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen.html. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2017): Cybersecuritybeeld Nederland. Available at: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2017): International One Conference 2017 – We are all connected. Available at: https://www.ncsc.nl/english/conference. Accessed 30 May 2017

Nationaal Cyber Security Centrum (2017): Whitepapers. Available at: https://www.ncsc.nl/actueel/whitepapers. Accessed 30 May 2017

6. OTHER SOURCES

Accenture and HfS Research (2016): The State of Cybersecurity and Digital Trust 2016 - Identifying Cybersecurity Gaps to Rethink State of the Art. Available at: https://www.accenture.com/us-en/new-applied-now. Accessed 16 May 2017

European Commission (2012): Decentralised Agencies – Overhaul – Analytical Fiche No3 – Agencies' seat and role of the host country. Available at: http://europa.eu/european-union/sites/europaeu/files/docs/body/fiche_3_sent_to_ep_cons_2010-12-15_en.pdf. Accessed 30 May 2017

Court of Auditors (2015): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2014 together with the Agency's reply. Available at: http://www.eca.europa.eu/Lists/ECADocuments/ENISA_2014/ENISA_2014_EN.pdf. Accessed 30 May 2017

Court of Auditors (2016): Report on the annual accounts of the European Union Agency for Network and Information Security for the financial year 2015 together with the Agency's reply; 2016/C 449/25

Court of Auditors (2016): Summary of results from the Court's annual audits of the European Agencies and other bodies for the financial year 2015; 2016/C 449/01

European Commission (2015): Commission Staff Working Document - Better Regulation Guidelines, SWD(2015) 110 final

European Commission (2015): Draft General Budget of the European Union for the financial year 2016 - Working Document Part III; COM(2015) 300

European Commission (2016): Digital Single Market, Pillar III: Trust & Security. Available at: https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security. Accessed 30 May 2017

European Commission (2016): The EU Single Market – Copyright and Neighbouring Rights - The EU legal framework ("acquis"). Available at: http://ec.europa.eu/internal_market/copyright/acquis/index_en.htm. Accessed 30 May 2017

European Cyber Security Organisation (2016): European Cyber Security cPPP Strategic Research & Innovation Agenda. Available at: https://ecs-org.eu/documents/ecs-cppp-sria.pdf. Accessed 30 May 2017

EY (2015): Cybersecurity and the Internet of Things. Available at: www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf. Accessed 16 May 2017

Georgian Institute of Technology (2016): 2016 Emerging Cyber Threats Report. Available at: www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf. Accessed 16 May 2017

Government of the Netherlands and Netherlands Organisation for Scientific Research (2013): National cybersecurity research agenda II. Available at: https://www.ncsc.nl/binaries/content/documents/ncsc-nl/expertise--advies/onderzoek-innovatie-en-onderwijs/1/NCRSA%2BII.pdf. Accessed 30 May 2017

PoliceMediaBlog (2016): Social Media Handbook for Law Enforcement – Europol EC3. Available at: https://policemediablog.com/2016/01/27/social-media-handbook-for-law-enforcement-europol-ec3/. Accessed 30 May 2017

The Kosciuszko Institute (2015): Strategic Perspectives on Cybersecurity Management and Public Policies. European CyberSecurity Journal (2015), Volume 1, Issue 1. Available at: https://app.box.com/s/hmvkjazr1jxppjgj3skkm31dl0k6lyxw. Accessed 16 May 2017

**APPENDIX 3
SURVEY QUESTIONNAIRES**

QUESTIONNAIRE ON ENISA'S GOVERNANCE, ORGANISATIONAL STRUCTURE AND WORKING PRACTICES

Thank you for taking the time to respond to this survey which will take approximately 15 to 20 minutes to complete.

What is this about?
This survey is carried out by Ramboll Management Consulting and Carsa in the context of the "Evaluation of ENISA 2013-2016" commissioned by DG CONNECT.

Who should answer?
The survey invites all ENISA staff and representatives to provide their assessments.
Please note that this survey is strictly confidential - your identity will not be disclosed and the survey will be anonymous.

How will this survey make a difference?
The survey data will contribute to the evaluation of ENISA over the 2013-2016 period and the identification of recommendations for the future. We would therefore highly appreciate your feedback.

Should you wish to read through the questionnaire prior to answering it, you may generate a printable version by clicking on this icon. You must, however, still **respond to the survey online.**

BACKGROUND QUESTIONS

Please describe your main relationship with ENISA?

(2)   ❑ ENISA Staff (including management)

(3)   ❑ ENISA Management Board

(4)   ❑ ENISA Executive Board

(5)   ❑ National Liaison Officer

(6)   ❑ Permanent Stakeholder Group

Which department do you work for within ENISA? (optional)

(1)   ❑ Stakeholder relations and administration

(2)   ❑ Core Operations

(3)   ❑ Other

Which entity do you represent? (optional)

(1)   ❑ The European Commission

(2)   ❑ An EU Member State

(3) ❑ An EFTA Country

(4) ❑ Other

From which location do you work? (optional)

(1) ❑ Heraklion

(2) ❑ Athens

How long have you been working for ENISA? (optional)

(1) ❑ <1 year

(2) ❑ 1-3 years

(3) ❑ 4-5 years

(4) ❑ 6-10 years

(5) ❑ > 10 years

ENISA'S ORGANISATIONAL SET-UP

To what extent do you agree/disagree with the statements below regarding ENISA?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
The size of the agency is appropriate for the work entrusted to ENISA and adequate for the actual workload.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
The organisational solutions and procedures of ENISA are well adapted to the work entrusted to it and to the actual workload.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
The staff composition is appropriate for the work	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
entrusted to ENISA and adequate for the actual workload.					
The recruitment and training procedures are appropriate for the work entrusted to ENISA and adequate for the actual workload.	(1) ☐	(2) ☐	(3) ☐	(4) ☐	(5) ☐

Please elaborate on your assessment of the statement "The size of the agency is appropriate for the work entrusted to ENISA and adequate for the actual workload."

_____

Please elaborate on your assessment of the statement "The organisational solutions and procedures of ENISA are well adapted to the work entrusted to it and to the actual workload."

_____

Please elaborate on your assessment of the statement "The staff composition is appropriate for the work entrusted to ENISA and adequate for the actual workload."

_____

Please elaborate on your assessment of the statement "The recruitment and training procedures are appropriate for the work entrusted to ENISA and adequate for the actual workload."

_____

To what extent do you agree/disagree with the statements below regarding the efficiency and/or effectiveness of ENISA's governance and management?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives).	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the efficient functioning of the Agency (i.e. in terms of value for money).	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
The establishment of an Executive Board has led to a more efficient functioning of the Management Board.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
ENISA's management practices are conducive to creating an effective organisation (i.e. in terms of	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
meeting its objectives).					
ENISA's management practices are conducive to creating an efficient organisation (i.e. in terms of value for money).	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
ENISA's location enables it to effectively conduct its work (i.e. in terms of meeting its objectives).	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
ENISA's location enables it to conduct its work efficiently (i.e. in terms of value for money).	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Please elaborate on your assessment of the statement "The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the effective functioning of the Agency (i.e. in terms of meeting its objectives)."

‾‾‾‾‾

Please elaborate on your assessment of the statement "The current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the efficient functioning of the Agency (i.e. in terms of value for money)."

‾‾‾‾‾

Please elaborate on your assessment of the statement "The establishment of an Executive Board has led to a more efficient functioning of the Management Board."

‾‾‾‾‾

Please elaborate on your assessment of the statement "ENISA's management practices are conducive to creating an effective organisation (i.e. in terms of meeting its objectives)."

_____

Please elaborate on your assessment of the statement "ENISA's management practices are conducive to creating an efficient organisation (i.e. in terms of value for money)."

_____

Please elaborate on your assessment of the statement "ENISA's location enables it to effectively conduct its work (i.e. in terms of meeting its objectives)."

_____

Please elaborate on your assessment of the statement "ENISA's location enables it to conduct its work efficiently (i.e. in terms of value for money)."

_____

ENISA'S EFFECTIVENESS AND EFFICIENCY

To what extent do you agree/disagree with the statements below regarding ENISA?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
ENISA's working practices are efficient and make best use of available resources.	(1) ❏	(2) ❏	(3) ❏	(4) ❏	(5) ❏
The internal capacity and capabilities of staff are well utilised in ENISA.	(1) ❏	(2) ❏	(3) ❏	(4) ❏	(5) ❏
Internal management systems for planning, follow-up and monitoring are	(1) ❏	(2) ❏	(3) ❏	(4) ❏	(5) ❏

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
effective (i.e. in terms of meeting its objectives).					
Internal management systems for planning, follow-up and monitoring are efficient (i.e. in terms of value for money).	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Knowledge and information sharing within ENISA are supported and encouraged.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
The administrative systems in place to support ENISA's operations are adequate and appropriate.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
The quality control mechanisms in place ensure a high and consistent quality in ENISA's work and publications.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Please elaborate on your assessment of the statement "ENISA's working practices are efficient and make best use of available resources."

_____

Please elaborate on your assessment of the statement "The internal capacity and capabilities of staff are well utilised in ENISA."

_____

Please elaborate on your assessment of the statement "Internal management systems for planning, follow-up and monitoring are effective (i.e. in terms of meeting its objectives)."

_____

Please elaborate on your assessment of the statement "Internal management systems for planning, follow-up and monitoring are efficient (i.e. in terms of value for money)."

_____

Please elaborate on your assessment of the statement "Knowledge and information sharing within ENISA are supported and encouraged."

_____

Please elaborate on your assessment of the statement "The administrative systems in place to support ENISA's operations are adequate and appropriate."

_____

Please elaborate on your assessment of the statement "The quality control mechanisms in place ensure a high and consistent quality in ENISA's work and publications."

_____

COOPERATION WITH STAKEHOLDERS

To what extent do you agree/disagree with the statements below regarding ENISA's cooperation with stakeholders?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
ENISA's activities are coherent with the policies and activities of its stakeholders.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
ENISA has built strong and trustful relationships with its stakeholders when executing	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
its mandate.					
The collaboration between the Permanent Stakeholder Group and ENISA has functioned well.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
The collaboration between the Permanent Stakeholder Group and ENISA has allowed for greater efficiency.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
ENISA is open to cooperating with a variety of stakeholders, across different levels and sectors, to ensure best results.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
ENISA has good systems and procedures in place for stakeholder consultation and management.	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

Is there anything else that you would like to add in relation to ENISA's governance, organisational structure and working practices?

_____

Thank you very much for your contribution!

Click Finish to close the consultation.

Your answers have been saved. If you would like a printed copy of your answers, please click

the print button.

QUESTIONNAIRE ON ENISA'S RELATIONSHIP WITH CERTS/CSIRTS

Thank you for taking the time to respond to this survey which will take approximately 10 minutes to complete.

What is this about?

This survey is carried out by Ramboll Management Consulting and Carsa in the context of the project "Evaluation of ENISA" commissioned by DG CONNECT.

Who should answer?

The survey invites CERTs / CSIRTs staff who have been sent a link to the survey to provide their assessments.

Please note that this is a strictly confidential survey - your identity will not be disclosed and the survey will remain anonymous.

How will this survey make a difference?

The survey data will contribute to the evaluation of ENISA over the 2013-2016 period and the identification of recommendations for improvement. We would therefore highly appreciate your feedback.

Should you wish to read through the questionnaire prior to answering it, you may generate a printable version by clicking on this icon. You must, however, still **respond to the survey online**.

BACKGROUND QUESTIONS

Can you briefly describe your main responsibilities?

(1) ❑ Preventative Measures (e.g. Penetration Testing)

(2) ❑ Incident Response Team

(3) ❑ Post Incident Management (e.g. Disaster Recovery)

(4) ❑ Customer Relationship Management

(5) ❑ Policy Development

(6) ❑ Public Awareness

(7) ❑ Administration and Management

(8) ❑ Other

Please describe which other responsibilities you are referring to:

_____

COHERENCE

To what extent did ENISA proactively support cooperation among CERTs / CSIRTs during the 2013-2016 period?

(1) ❑ Not at all

(2) ❑ To a limited extent

(3) ❑ To some extent

(4) ❑ To a high extent

(5) ❑ Do not know

What else do you think could be done by ENISA to improve cooperation among CERTs / CSIRTs?

_____

To what extent did ENISA cover CERTs / CSIRTs' needs over the 2013-2016 period?

(1) ❑ Not at all

(2) ❑ To a limited extent

(3) ❑ To some extent

(4) ❑ To a high extent

(5) ❑ Do not know

In your opinion, how important were ENISA's capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) in 2013-2016 for CERTs / CSIRTs' development?

(1) ❑ Not at all

(2) ❑ Of limited importance

(3) ❑ Important

(4) ❑ Very important

(5) ❑ Do not know

To what extent will the new role foreseen for ENISA in relation to CERTs / CSIRTs as part of the NIS Directive enable ENISA to better cover CERTs / CSIRTs' needs?

(1) ❑ Not at all

(2) ❑ To a limited extent

(3) ❑ To some extent

(4) ❑ To a high extent

(5) ❑ Do not know

In concrete terms, what do you foresee ENISA doing as part of its new role as secretariat for the CSIRTs Network, as foreseen in the NIS Directive?

_____

What else do you think could be done by ENISA to better cover CERTs / CSIRTs' needs?

_____

DEGREE OF COHERENCE AND COMPLEMENTARITY

The activities below were activities conducted by ENISA to support CERTs/CSIRTs over the 2013-2016 period. In your opinion, to what extent were these activities coherent with and complementary to (i.e. not overlapping or duplicating) what CERTs/CSIRTs were doing?

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
Organising and managing large-scale cyber security exercises	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Creating tools and best practices	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Providing training courses	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Developing training methodologies	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
Creating training and exercise material	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Developing publications	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Working towards cyber security cooperation	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Providing guidance based on best practice in the area of operational community efforts (operational cooperation, information exchange, etc.)	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Creating reports and roadmaps	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Organising workshops and conferences	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Supporting cooperation among CERTs/CSIRTs, within the CERTs/CSIRTs network	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑
Contributing to the dialogue between CERTs / CSIRTs and law enforcement and data privacy communities, in order to support consistent a EU-wide approach to NIS	(1) ❑	(2) ❑	(3) ❑	(4) ❑	(5) ❑

	Not at all	To a limited extent	To some extent	To a high extent	Do not know
Supporting the collaboration between CERTs / CSIRTs and law enforcement communities, in responding to recent policy and technical developments in this area	(1) ❏	(2) ❏	(3) ❏	(4) ❏	(5) ❏

Is there anything else that you would like to add?

_____

Thank you very much for your contribution!

Click Finish to close the questionnaire. Your answers have been saved. If you would like a printed copy of your answers, please click the print button.

**APPENDIX 4
POSITIONING EXERCISE**

This appendix presents the detailed assessment of activities of ENISA and other national and EU bodies prepared for the positioning exercise. These tables have been prepared based on findings from desk-based research and interviews with the concerned organisations. They provide an assessment on whether activities implemented by ENISA are also implemented by other EU or national bodies and if so, whether this represents a complementarity or an overlap.

The following EU bodies/organisations have been covered in the positioning exercise:
- CERT-EU (information confirmed by the organisation)
- Europol – EC3 (based on desk research)
- DG JRC (information confirmed by the organisation)

At national level, three organisations were covered:
- INCIBE – Spain (based on desk research)
- National Cyber Security Centre – Netherlands (information confirmed by the organisation)
- ANSSI – France (based on desk research)

Note on methodology

ENISA's activities were mapped for the positioning exercise as presented in the table below.

Table 30: Overview of positioning analysis framework

Overarching theme	ENISA's activities	Sub-activity
To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	Creation of good practices and recommendations on the security and resilience of	Critical Infrastructures
		Transportation
		Health
		Energy (incl. Smart grids)
		Homes
		Finance
		Big Data
		Recommendations on aligning research programme(s) with policy in the specialised area of NIS
	Regular threat analysis reports	Covering the themes described above (critical infrastructures, transportation, etc.)
		Annual overall threat analysis/landscape report
		Threat analysis reports specific for governments
		Threat analysis reports specific for SMEs
		Threat analysis reports specific on NIS issues
	Knowledge and methodology enhancement	Increase in cryptographic knowledge
		Identifying critical communication networks, links, and components
To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security	Good practices, reports and standardisation for legal and policy areas	Provide an overview of the threat landscape for the legal framework
		Provide best practices for data protection legal framework
		Provide best practices for incident handling legal framework
		Contribute to the development and implementation of the NIS directive
		Provide good practices for cryptographic protection measures
		Provide guidance for harmonisation of legal framework and standards for the private sector
		Support policy discussion in thematic areas: -smart grids -IT security certification -finance -electronic communications
To assist the Member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	Good practices, white papers and guidelines	on how to conduct risk assessment and handle incident tracking
		on how to conduct training and exercises
		directed towards vulnerable infrastructures
		related to NIS Directive needs
		for fostering cybersecurity culture in the private sector
		for national cybersecurity strategies

	Trainings	Trainings and exercises for CERTs
		On-request training for Member States and EU bodies
		Workshops to Assist and advise Member States on the secure use of cloud computing for e-government applications and services
		On-request support for Member States decision-making in the areas of privacy and trust
	Standardisation	Harmonised Minimum Security Measures for Internet Service Providers
		Provide minimum Security Measures for Cloud Computing
	Direct support and assistance	Provide guidance and support for the European Cyber Security Month
		Support the working groups of the NIS platform
		Direct support for CERTs strategic direction
		Assisting member states in building capabilities on national Private-Public-Partnerships (PPPs)
		Support and advise member states on the establishment and evaluation of national cybersecurity strategies
	Incident analysis	Annual incident reports and recommendations on how to mitigate threats
To enhance cooperation both between the Member States of the European Union and between related network and information security communities	Cross Member States cooperation building	Workshops with 2 or more Member States
		Fostering discussion among 2 or more Member States through events
		Cybersecurity exercises with 2 or more Member States

to the aim of this exercise was to compare ENISA's services with those of CERT-EU, EC3, DG JRC, the Dutch National Cyber Security Centre, the French National Cybersecurity Agency and the Spanish National Institute for Cybersecurity. In order to do so a desk research was conducted and individuals in the concerned organisations were contacted to gather the missing information. A full assessment of overlaps and complementarities was provided by CERT-EU and a partial contribution was received from the DG JRC, Netherlands National Cyber Security Centre and the Spanish National Institute for Cybersecurity (providing detailed information on activities but with no assessment of overlaps or complementarities). For the remaining organisations (EC3 and the French ANSSI) best judgments were made regarding possible overlaps or complementarities given the limited information available online.

Organisations were compared at the activity level based on an overall assessment of the differences or similarity observed between organisations. Finally, desk research findings were cross-checked with information obtained from the interviews. Based on this research complementarities and overlaps were identified.

It is to be noted that even if no clear overlap was identified, the issue might remain that ENISA does not build on the existing competencies and activities of other organisations. For example, even if reports produced by ENISA do not cover exactly the same topics as reports produced by other organisations, it might be the case that there is room for more efficiency gains in ENISA not basing is work on the existing work done in other organisations on the topic.

1. CERT-EU

All information provided in the comments concerning CERT-EU's activities was provided directly by CERT-EU through the positioning exercise and the interviews.

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	Good practices and recommendations	Complementarity	CERT-EU contributes to ISACs related to critical infrastructure, transportation, health and other topics relevant to the thematic areas of focus of ENISA. They provide information about the technical developments in the threat landscape and offer informal security advice. They service therefore complements that of ENISA. As pointed out during an interview, there is a risk that CERT-EU and ENISA publish statements on issues already covered by one another but this risk does not represent an actual overlapping issue.
	Regular Threat Analysis Reports	Complementarity	CERT-EU provides highly technical reports aimed at its constituents and peers and include non-public information which is distributed on a need-to-know basis. ENISA's reports contain only public information and are written for the public at large. They therefore complement each other. In addition, CERT-EU uses the reports produced by ENISA for their own monthly reports and feed into ENISA's annual report. They try to have an operational cooperation and avoid any duplication of work.
	Knowledge and Methodology Enhancements	Complementarity	CERT-EU provides limited advice to its constituents on how to identify critical communication networks, links and components. ENISA works for the public at large. They therefore complement each other. One interview pointed at the danger for overlap in the work CERT-EU and ENISA conduct on cryptography and vulnerabilities.[141]
To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security	Good practices, reports and standardisation for legal and policy areas	Complementarity	CERT-EU brought out guidelines for notifications of cyber-security incident response processes to Data Protection Officers, aimed at EU institutions, bodies and agencies but published as a white paper. They therefore aim at a different scope and audience than ENISA.
To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	Good practices, white papers and guidelines for the government	None	CERT-EU publishes white papers on selected security issues of current interest on their website, which are publicly available.
	Trainings	Complementarity	CERT-EU provides very technical trainings and workshops to its constituency. The audience differs from that of the trainings delivered by ENISA.
	Standardisation	None	N/A
	Direct Support and Assistance	Overlap	While CERT-EU discusses best practices with other CERTs, they do not provide direct support and assistance. It appeared however that those who want to build a CERT go to CERT-EU for practical advice rather than to ENISA. There is a risk of overlap in the advice and expertise that both organisations provide them with.
	Incident Analysis	Complementarity	CERT-EU provides incident analysis reports to its constituency. These reports are however highly technical, confidential

---

[141] We were not able to identify clear evidence for such overlaps in publicly accessible reports and have therefore not taken into account the evidence coming from this one interview.

			and exclusive to these constituents and peers. ENISA's incident analysis reports are public.
To enhance cooperation both between the Member States of the European Union and between related network and information security communities	Cross Member States cooperation building	Overlap	CERT-EU organised workshops on Malware Information Sharing Platforms in which national and governmental CERTs participated. Nine interviews pointed at the fact that CERT-EU tends to act outside of its mandate on cooperation building, potentially overlapping with what ENISA is or should be doing. For example, CERT-EU should not be directly getting in touch with commercial organisations in Member States but does so through national CERTs.

2. Europol – EC3

Little information is accessible on EC3's website. The assessment below was made by the evaluators but was not confirmed by EC3.

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	Good practices and recommendations	None	N/A
	Regular Threat Analysis Reports	None	N/A
	Knowledge and Methodology Enhancements	None	N/A
To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security	Good practices, reports and standardisation for legal and policy areas	Complementarity	EC3 works together with ENISA to provide workshops which aim at defining a common taxonomy between CSIRTs and Law Enforcement and facilitate information sharing between the two communities.[142] EC3 developed a Handbook for Law Enforcement on the use of social media for prevention/awareness purposes.[143]
To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	Good practices, white papers and guidelines for the government	None	N/A
	Trainings	Complementarity	EC3 supports training for the relevant authorities in Member States.[144] It however provides trainings that are very focused on reacting to cybercrime by involving the national law enforcement authorities, therefore differing from what ENISA does.
	Standardisation	None	N/A
	Direct Support and Assistance	Complementarity	EC3 provides direct support in reducing cybercrime through its operational powers (e.g. arresting cyber criminals or taking down cybercrime forums).[145]
	Incident Analysis	Complementarity	EC3 does not provide publicly available incident analysis reports but has some publicly available tools to understand the different types of cyber threats and how individuals can avoid becoming victims to them.[146]
To enhance cooperation both between the Member States of the European Union and between	Cross member states cooperation building	Complementarity	As noted previously, EC3 works together with ENISA to provide workshops which aim at defining a common taxonomy between CSIRTs and Law Enforcement

---

[142] https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop
[143] https://policemediablog.com/2016/01/27/social-media-handbook-for-law-enforcement-europol-ec3/
[144] https://www.europol.europa.eu/activities-services/services-support/training-and-capacity-building
[145] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-2
[146] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-2

| | | | and facilitate information sharing between the two communities.[147] |

3. DG JRC

All information provided in the comments concerning the DG JRC's activities was provided directly by the DG JRC through the positioning exercise and the interviews.

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	Good practices and recommendations	General complementarity but some risk for duplication	The DG JRC provides good practices and recommendations on critical infrastructures, transportation, energy and homes. These activities primarily come in form of a contribution to the Commission's work and are in this sense complementary to ENISA's work targeting Member States and a broader stakeholder group.

E.g. contribution to Commission work on Cooperative Intelligent Transport System (C-ITS), in particular with respect to security and privacy: participation in the C-ITS platform, contribution to its final report, to the preparation of the "European Strategy for C-ITS" Com(2016)-766, to the C-ITS common certificate and security policy, Interaction as Commission representative with the Technology subgroup of the Article 29 working party

Preparation of a BREF (Best Available Techniques Reference Document) for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems. Co-chairing with DG ENER of the WG2 (on cybersecurity and privacy) of the Smart Grid Task Force |
| | Regular Threat Analysis Reports | Complementarity | Through the ITIS project, DG JRC provides news bulletins on vulnerabilities and threats in the EU for the energy sector and also half year reports on foresight for emerging threats |
| | Knowledge and Methodology Enhancements | Risk of duplication | The DG JRC has developed risk assessment methodologies reports that are available to the MS for implementation |
| **To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security** | Good practices, reports and standardisation for legal and policy areas | Complementarity | The DG JRC provides direct support to the European Commission in the development of good practices and standardisation for legal and policy areas. E.g. contribution to the recent review of the ePrivacy Directive and preparation of a proposed Regulation

Starting, supporting DG CNECT with methodology and best practices insights, in the NIS Cooperation Group, for Essential Services identification and the criteria to use. Work on the preparation of a roadmap for the security certification and labelling of ICT goods and services (part of COM(2016) 410 - Strengthening Europe's Cyber Resilience System) Request for DG CNECT to support the identification of essential services by MS. |
| **To assist the member States and the European Union institutions and bodies in enhancing** | Good practices, white papers and guidelines for the government | Complementarity | The DG JRC has developed risk assessment methodologies reports that are available to the MS for implementation |
| | Trainings | Complementarity | The DG JRC does not provide training to |

---

[147] https://www.enisa.europa.eu/events/5th-enisa-ec3-workshop

capacity building throughout the European Union			CERTs. Three training activities until now for MS and for operators of critical infrastructures in the EU. These are done on requests
	Standardisation	None	N/A
	Direct Support and Assistance	None	N/A
	Incident Analysis	None	N/A
To enhance cooperation both between the Member States of the European Union and between related network and information security communities	Cross member states cooperation building	Complementarity	Workshops on: zero-day vulnerability EU governance, Transborders personal data-breach exercise, data portability, encryption/decryption The DG JRC is supporting the EU Critical Information Infrastructure Protection (CIIP) Action Plan by contributing to the organisation of pan-European cyber-security exercises. This is organised in cooperation with ENISA.

4. INCIBE – Spain

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	Good practices and recommendations	Complementarity	INCIBE produces some guides aimed at public and private actors.[148] These guides and the guides produced by ENISA do not have obvious overlaps and can be used in a complementary fashion by end-users.
	Regular Threat Analysis Reports	Overlap	INCIBE compiles incidents notice and provides a number of incident analysis reports.[149] While these might be in Spanish and with a particular national focus, it is unclear whether the actors looking at these analyses benefit from the additional analysis reports provided by ENISA.
	Knowledge and Methodology Enhancements	Overlap	INCIBE helps companies in critical infrastructures to identify critical weaknesses.[150] It is unclear what additional value ENISA is bringing to these companies when they provide help on identifying critical communication networks, links and components. There were no clear overlaps identified concerning other areas of knowledge and methodology enhancements.
To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security	Good practices, reports and standardisation for legal and policy areas	Complementarity	INCIBE cooperates with the Spanish government to produce standardised best practices which aim at contributing to the development and implementation of the NIS Directive. They have for example compiled all of the Spanish legislation which affects the area of cybersecurity.[151] ENISA brings in the EU aspect and helps INCIBE and the Spanish government by providing what they see as being the best practices based on experience across Member States.
To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	Good practices, white papers and guidelines for the government	Complementarity	INCIBE produces a number of reports which aim at providing best practices, for example on how to conduct trainings and exercises[152], how businesses should manage risks[153]. In addition, they work alongside the Spanish government on establishing national strategies related to the NIS Directive.[154] ENISA's complementary role here is to

---

[148] https://www.incibe.es/protege-tu-empresa/guias
[149] https://www.certsi.es/servicios-operadores/notificaciones-y-analisis-adhoc
[150] https://www.certsi.es/servicios-operadores/detector-de-incidentes
[151] http://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Ciberseguridad
[152] https://www.certsi.es/guias-y-estudios/estudios/taxonomia-ciberejercicios
[153] https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf
[154] https://www.incibe.es/sala-prensa/notas-prensa/nw-infoday-raul-riesco

	Trainings	Complementarity	INCIBE provides trainings and exercises, including to CERTS and security forces[155][156]. It seems that ENISA focuses more on capacity building trainings for CERTs and that INCIBE provides specific trainings (e.g. on fraud detection using machine learning and deep learning).[157]
			link this effort with the good practices observed at the European level.
	Standardisation	None	INCIBE does not seem to provide minimum security measures to internet service providers or for cloud computing in the same way ENISA does.
	Direct Support and Assistance	Complementarity	INCIBE provides some support to the state on establishing and evaluating its National Cyber Security Strategy and contributes to the establishment of private-public partnerships in cybersecurity.[158] It is however unclear how much of what they do is complementary or overlapping with ENISA's activities. We did not identify any clear overlaps.
	Incident Analysis	Overlap	INCIBE repertories and analyses incidents happening in Spain.[159] They also provide advice to companies on how to mitigate threats and identify their own weaknesses.[160] It is therefore unclear what ENISA's added value is in that regards.
To enhance cooperation both between the Member States of the European Union and between related network and information security communities	Cross member states cooperation building	Complementarity	INCIBE organises workshops[161] and helps foster discussion among member states[162] with the help and in coordination with ENISA.

5. NCSC - Netherlands

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
To develop and maintain a high level of expertise of European Union actors, taking into account evolutions in network and information security	Good practices and recommendations	Overlap	The Dutch Cybersecurity Centre produces good practices for critical infrastructures and for the protection of home internet devices.[163] It is not clear what the added value of good practices produced in these areas by ENISA would have in the Netherlands.
	Regular Threat Analysis Reports	Overlap	The Dutch Cybersecurity Centre compiles incidents and provides regular threat analysis reports. These reports are in Dutch and seem to focus on the national level.[164] It is however not clear what the added value of the reports provided by ENISA is for the Dutch actors.
	Knowledge and Methodology Enhancements	Complementarity	The Dutch Cybersecurity Centre conducts research in cryptography.[165] No clear overlap was spotted between the reports produced by the Dutch Cybersecurity Centre and the ones produced by ENISA.
To assist the Member States and the European Union institutions and	Good practices, reports and standardisation for legal and policy areas	Overlap	The Dutch Cybersecurity Centre produces a number of reports and white papers[166] to support the government of the

---

[155] https://cybercamp.es/summer-bootcamp
[156] https://www.incibe.es/formacion
[157] https://cybercamp.es/programa/agenda
[158] https://ecs-org.eu/documents/ecs-cppp-sria.pdf
[159] https://www.certsi.es/alerta-temprana/avisos-sci
[160] https://www.certsi.es/servicios-operadores/detector-de-incidentes
[161] https://www.incibe.es/en/enise
[162] https://www.incibe.es/sala-prensa/notas-prensa/el-instituto-nacional-ciberseguridad-representa-los-intereses-nacionales-el
[163] https://www.ncsc.nl/actueel/factsheets/checklist-beveiliging-van-ics-scada-systemen.html
https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-apparaten-gekoppeld-aan-internet.html
[164] https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland
[165] https://www.ncsc.nl/binaries/content/documents/ncsc-nl/expertise--advies/onderzoek-innovatie-en-onderwijs/1/NCRSA%2BII.pdf
[166] https://www.ncsc.nl/actueel/whitepapers

			Netherlands on the topic of the cybersecurity legal framework. It is unclear how much ENISA is bringing in addition to the work already happening.
bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network and information security			
To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	Good practices, white papers and guidelines for the government	No	The Dutch Cybersecurity Centre did not report any activity in this category.
	Trainings	Overlap	The Dutch Cybersecurity Centre provides trainings and exercises such as the ISIDOOR exercise. Their audience includes some CERTs. There is therefore a risk of overlap here depending on the content of each training.
	Standardisation	No	The Dutch Cybersecurity Centre did not report any activity in this category.
	Direct Support and Assistance	No	The Dutch Cybersecurity Centre did not report any activity in this category.
	Incident Analysis	Overlap	The Dutch Cybersecurity Centre produces an annual cybersecurity report for the Netherlands[167]. It is unclear how useful the annual cybersecurity landscape report by ENISA is useful to the Netherlands. It might be good for cross-referencing and providing additional details.
To enhance cooperation both between the Member States of the European Union and between related network and information security communities	Cross member states cooperation building	Complementarity	The Dutch Cybersecurity Centre organises yearly conferences called the International One Conference[168]. They also organise cyber exercises with neighbouring countries. As such, they participate in the same effort as ENISA towards cooperation building without duplicating what ENISA does.

6. ANSSI - France

Category of Activity	Sub-Category of Activities	Overlap / Complementarity	Comment / Example
To develop and maintain a high level of expertise of European actors, taking into account evolutions in network and information security	Good practices and recommendations	Overlap	There might be some overlaps in that ANSSI provides good practices for individuals[169], industries[170] and administrations[171]. While these good practices might be in French or focused on the French national context, there is a risk of duplication of work if ENISA produces similar good practices.
	Regular Threat Analysis Reports	Overlap	ANSSI regularly provides threat analysis to inform individuals, governments and enterprises of the threat landscape.[172] It produces reports on the different techniques used by cyber criminals.[173] While these reports might be in French, if they are made publicly available, there is therefore a risk of overlap with what ENISA is doing,
	Knowledge and Methodology Enhancements	Overlap	ANSSI does quite a lot of work on cryptography.[174] There is therefore a risk of overlap with what ENISA does in that regard.
To assist the Member States and the European Union institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of network	Good practices, reports and standardisation for legal and policy areas	Complementarity	ANSSI provides advice to the French government on strategies to take and best practices to observe in order to foster cybersecurity in France.[175] ENISA is however complementary to that work in that they support the development of EU policies and represent the interest of ANSSI and other CS agencies in dialogues

---

[167] https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland
[168] https://www.ncsc.nl/english/conference
[169] https://www.ssi.gouv.fr/particulier/bonnes-pratiques/
[170] https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
[171] https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[172] https://www.ssi.gouv.fr/entreprise/principales-menaces/
[173] https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf
[174] https://www.ssi.gouv.fr/entreprise/actualite/crypto-le-webdoc/
[175] https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf

and information security			among the EU institutions in supporting the implementation of EU legislation. This was noted during the interview with ANSSI as a new need identified by the French agency.
To assist the member States and the European Union institutions and bodies in enhancing capacity building throughout the European Union	Good practices, white papers and guidelines for the government	Overlap	ANSSI has a number of good practices aimed at the public[176] and the private sectors.[177] They also work with the government to define strategies related to the NIS Directive needs.[178] There is therefore a risk of overlap with what ENISA is doing.
	Trainings	None	N/A
	Standardisation	Overlap	ANSSI aims at enforcing standards through the creations of qualifications and certifications in France.[179] There is therefore a risk of overlap with what ENISA does.
	Direct Support and Assistance	Complementarity	ANSSI is a campaign coordinator for the European Cyber Security Month.[180] It also provides direct support and assistance to the French government.[181] As such, it is complementary with what ENISA does.
	Incident Analysis	None	N/A
To enhance cooperation both between the Member States of the European Union and between related network and information security communities	Cross member states cooperation building	Complementarity	ANSSI works in collaboration with ENISA on organising and attending events which aim at increasing cooperation among member states.[182]

---

[176] https://www.ssi.gouv.fr/particulier/bonnes-pratiques/
[177] https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/
[178] https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf
[179] https://www.ssi.gouv.fr/entreprise/produits-certifies/
[180] https://www.ssi.gouv.fr/en/actualite/anssi-ready-for-the-2016-european-cybersecurity-month-escm/
[181] https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_2015_anssi.pdf
[182] https://www.ssi.gouv.fr/en/actualite/stronger-together-anssi-successfully-took-part-in-pan-european-exercice-cyber-europe-16/

APPENDIX 5
COMPREHENSIVE SWOT TABLE

STRENGTHS	WEAKNESSES
Independence / neutrality. ENISA is an independent agency without political or commercial bias. Its independence is supported by its location in Heraklion and Athens giving it less involvement in the everyday politics in cybersecurity in Brussels.[183]	**Lack of a more strategic, long-term vision.** ENISA has difficulties in executing a long-term vision due to regulatory constraints and overlapping mandates (other agencies/bodies claiming to have expertise and ownership in cybersecurity).[184] ENISA's work programme is influenced by the interests of Member States, although its flexibility has been broadened by Art.14, it's not enough.[185] [186]
Capacity building assistance. ENISA has a good track record / experience organizing trainings, cybersecurity exercises, development of manuals, studies trying to reach a broad sector (Member States, private actors, European Union institutions and agencies[187]). The aim of this capacity building activity is to develop the capabilities of the agents, providing them with the necessary tools to prevent, detect and handle incidents.[188] Agencies reporting best practices on the cyber domain could be encouraged.[189]	**Limited visibility of ENISA.** As a result of weak communication, marketing and/or branding, ENISA is not very present, i.e. it has not managed to carve out its own space within the cybersecurity policy landscape.[190]
Maintaining the network / coordination role[191]. ENISA is involved in addressing existing fragmentation at national, European and international level[192]. It acts as a pole to gather and exchange information and best practices among Member States, EU and international players. ENISA is also involved in fostering cooperation with the private sector and encourages the setup of PPP as a way to increase the operational capabilities in the sector. It also bolsters the establishment of cyber threat reporting channels as a way to	**Office location in Heraklion and Athens.** ENISA's location impacts its capabilities / capacities in terms of recruiting high-level experts (difficulties for spouses to integrate and limited international schooling options) and connectedness to influence cybersecurity policy in Brussels due to the distance to decision makers in the EU institutions. An option would be to have a liaison office.[195]

---

[183] See interviews

[184] See interviews

[185] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

[186] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

[187] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

[188] See European Parliament and Council Regulation (EU) No 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

[189] Experts discussions

[190] See interviews

[191] See European Parliament and Council Regulation (EU) No 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

[192] See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

gather information and disseminate expertise.[193] Furthermore, being part of the EC3 board assures ENISA involvement in other NIS related issues of cybercrime.[194]	
Member States support: ENISA has cyber resilience capability and supports the fostering of Member States' effectiveness in this area.[196] [197, 198] It also, plays a role assisting the national CERTs (from their set-up to their daily activities)[199]. Its role as CERT coordination should be enhanced.[200]	**Inadequate staff composition and human resources policies.[201]** ENISA's staff lacks the technical expertise to act as a reference in cybersecurity in policy. Next to a lack of computing specialists, there is a lack of carreer opportunities within the Agency. More junior staff members tend to move on causing capability loss of the Agency.
Horizontal policy expertise. ENISA has expertise and experience in strengthening detection and prevention of cybersecurity threats in different country contexts giving it more horizontal expertise. One of its main activities is to assist the development and implementation of NIS related policies and laws, trying to strengthen the importance of cybersecurity as an EU policy priority.[202]	**Limited size and low financial resources.[203]** The budget allocated for cybersecurity is low if compared with other areas or with the resources spent in other countries on this issue.[204]
Recognised relationships with its stakeholders. ENISA's stakeholders judge their relationship with ENISA to be trustful and effective.	**Recruitment and training procedures.** Recruitment and training procedures of ENISA are considered not appropriate or only appropriate to a limited extent to manage ENISA's workload. Additional comments revealed that the recruitment process is considered too slow and therefore not being adapted to the cybersecurity domain.[205]

[195] See interviews

[193] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

[194] See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee

[196] See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

[197] See ENISA (2016) Evaluation Roadmap 25/07/2016.

[198] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

[199] See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

[200] See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee

[201] See interviews

[202] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

[203] Ibid.

[204] See Fahey, E. (2014) 'EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security'. European Journal of Risk Regulation, Vol. 5, No. 1, pp. 46-60.

[205] See ENISA survey

OPPORTUNITIES	**THREATS**
Synergies & risk management culture[206]. There is a growing need to explore and ensure synergies between operators as to assure concerted and collaborative NIS policy actions[207]. Cooperation is also important in the public-private dimension. Improvement regarding information sharing could help the creation of a coherent risk management culture aligned with existing crisis mechanisms. ENISA could work to ensure effective cooperation and prompt information sharing between EU institutions and different agencies, national government and the private sector. Without the involvement of the private sector it will be difficult to identify the relevant threats.[208]	**Insufficient sharing of information - lack of data.** Stakeholders in the private sector are reluctant to share information regarding NIS incidents[209]. The fact that reporting is not mandatory for public authorities does not encourage the private sector to do so on a voluntary basis. In addition, some private companies lack training in cybersecurity issues[210]. Incentives for information disclosure are not attractive. Some sectors are more eager to cooperate than others (financial vs telecommunications). Member States are also averse to disclose relevant information to ENISA, in particular, where national security is concerned. Furthermore, there is a lack of consensus among Member States' understanding of the cyber domain[211] [212]
ICT standardization, certification and harmonisation. ENISA should encourage harmonisation regarding threat assessments (threats, threat tools and vulnerabilities). In order to create digital trust, ENISA should seek to introduce a European ICT labelling for cybersecurity products. This would help foster the integration of the Single Market, create trust and protect credentials. Harmonisation of different national legislation should be sought at EU level in order to have an effective cybersecurity protection.[213]	**Fragmentation and coordination**. Fragmentation is an issue regarding operational capabilities[214] (e.g. ENISA has no operational power and therefore cannot intervene to fix NIS issues)[215]. In addition, there is a diverse set of agencies dealing with different issues in the cyber incident landscape. Coordination amongst different agencies is sometimes not only difficult, but also distorts the visibility and hinders accessibility of the European response to threats and demands of

---

[206] See European Commission (2013). SWD (2013) 31 final; COM (2013) 48 final: Commission Staff Working Document-Executive Summary of the Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union.

[207] See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

[208] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

[209] See European Commission (2013). SWD (2013) 31 final; COM (2013) 48 final: Commission Staff Working Document-Executive Summary of the Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union.

[210] See European Commission (2013). JOIN (2013) 1 final: 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: An Open, Safe and Secure Cyberspace

[211] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

[212] See Carrapico, H., Barrinha, A. (2017). The EU as a coherent (cyber)security actor?

[213] See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee

[214] See ENISA (Jan 2016). ENISA Strategy 2016-2020, Catalogue number TP-04-16-453-EN-N; ISBN: 978-92-9204-170-0

	stakeholders. For instance, one Member State representative claimed that "his organisation did not work together with ENISA and that if they came across ENISA's work, it was by coincidence"[216]. There is a need to disseminate ENISA's work. Furthermore, a clear distribution of competences within the different agencies could help to strengthen EU capacity to react.[217] Some experts suggest that if similar functions are identified at ENISA, EC3 or CERT-EU they should be merged.[218]
Awareness raising and capacity building. Public awareness on cyber threats should be enhanced. ENISA could enhance its discourse and awareness strategy and provide additional guidance, training regarding management of cyber threats.[219] ENISA could also use its expertise in cyber resilience to strengthen pan-European cyber incident exercises and examine computer security incident response teams.[220] There is a need to assist and develop national cyber resilience capability and ENISA should continue its works in the domain, helping for instance the development of national contingency plans and organizing regular emergency exercises and setting alarms to detect attacks on critical infrastructures.[221]	**Cooperation with Member States - capability gaps.** The priorities set by national governments in cybersecurity vary significantly among Member States. Member States' cyber capacities and capabilities are uneven[222] [223] not only at preparedness level, but also at policy. Divergent legislation, priorities and coordination problems can lead towards Single Market fragmentation, lack of effectiveness of the European response and interoperability problems when incidents spread across borders.[224] The new Cooperation Group set up by NIS Directive, aims to overcome this weakness aiming to strengthen cooperation among Member States and offering advice on security issues.[225]

---

[215] See European Commission (2013). JOIN (2013) 1 final: 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: An Open, Safe and Secure Cyberspace

[216] See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

[217] See ENISA (2016) Evaluation Roadmap 25/07/2016.

[218] See Fahey, E. (2014) 'EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security'. European Journal of Risk Regulation, Vol. 5, No. 1, pp. 46-60.

[219] See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

[220] Ibid.

[221] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

[222] See European Commission (2013). JOIN (2013) 1 final: 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: An Open, Safe and Secure Cyberspace

[223] See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

[224] See European Commission (2013). SWD (2013) 31 final; COM (2013) 48 final: Commission Staff Working Document-Executive Summary of the Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high level of network and information security across the Union.

[225] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

| Stakeholder engagement.
Reinforce links with industry stakeholders[226]. Broader cybersecurity ecosystem.
Sharing of information, practices among operators → instrumental role of ENISA.[227]
EU agencies are one of the principal channels to engage with the private sector.[228] | Lacking capacities to respond to changing technological landscape and corresponding new vulnerabilities[229], such as:
• Data theft of corporate information: emergence of "corporate insider"
• Economic espionage and state sponsored activities
• Overall data loss or destruction
• Malicious apps (malware)
• Hijacking-interception of information
• Nefarious activity: identity fraud, denial of service, malicious code, rouge certificates, failure of business process
• Online fraud-point

Cyber-attack methods have become more pervasive[230] → low-end, low to medium tech. Furthermore, cyber-attackers' profile, methods, and aims are diverse. It is not possible do draw an accurate portrait.

In addition, states are not only subject to cyber-attacks but are also performing them. The EU is lacking a method to detect and disseminate information about threats and attacks.[231] |
| Multi-perspective and holistic approach.
There is a need for comprehensive security policies. Broader engagement from industry and the community should be envisaged, as well as the use of dual capabilities (e.g. civil-military cooperation)[232]. Civil society perspective should also be taken into account.[233]

If incident report becomes mandatory for other sectors, there can be new opportunities for ENISA to support Member States in building | Internet of Things (IoT). Interconnectivity between devices implies that there is a larger vulnerable surface.[235] The boundary of the companies is disappearing as everything is connected, and thus finding loopholes to enter is easier. Securing the supply chain is still challenging.[236] |

[226] See European Commission (2013). JOIN (2013) 1 final: 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: An Open, Safe and Secure Cyberspace

[227] See ENISA (2015). Threat Landscape and Good Practice Guide for Software Defines Networks/ 5G: ISBN: 978-92-9204-161-8, DOI: 10.2824/67261.

[228] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

[229] See European Commission (2013). JOIN (2013) 1 final: 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: An Open, Safe and Secure Cyberspace

[230] See ENISA (2015). CYBER 7: Seven messages to the edge of Cyber-Space; Catalogue Number: TP-04-15-745-EN-C; ISB: 978-92-9204-133-5.

[231] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

[232] See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry.

[233] The Kosciuszko Institute- European CyberSecurity Journal (2015), Volume 1, Issue 1. Strategic Perspectives on Cybersecurity Management and Public Policies

more resilience against cyber-attacks. Without carefully defined and orchestrated security rules and procedures, it is impossible to imagine a functional and reliable software-defined networking infrastructure.[234]	
Consumer protection. Safeguard online environment providing highest possible freedom and security (fundamental rights, freedom of expression, personal data and privacy).	**Talent Gap.** There are not enough cybersecurity skilled workers → There is a need to broaden the pool of talent. [237, 238]
Cross-border coordination. As most of the incidents arise from cross border activity, ENISA could strengthen its coordination role at EU level.[239] [240] The EU level is best placed to supervise and respond to cyber-attacks, in order to help close the capability gaps that are identified at national level.[241]	**Lack of funding and prioritisation of cybersecurity at enterprise level.** There is not enough available funding for private companies to secure their infrastructure[242, 243] Private companies also often do not set cybersecurity as a clear priority (statement from experts) – lack of interest to invest in cybersecurity.[244]
The **NIS Directive** has helped to develop a coherent and less fragmented vision of cybersecurity at EU level.[245]	**NIS Directive - additional tasks, but no extra funding.[246]** The NIS Directive imposes many additional tasks on the Agency without cuts on responsibilities assigned before the NIS Directive. At the same time, no increase in the resources occurred. There is a risk that ENISA will not be able to deliver high quality outputs on all the tasks entrusted to it.

[235] See ENISA (2015). CYBER 7: Seven messages to the edge of Cyber-Space; Catalogue Number: TP-04-15-745-EN-C; ISB: 978-92-9204-133-5.

[236] Georgian Institute of Technology (2016). 2016 Emerging Cyber Threats Report.

[234] European Commission (2015). COM (2015) 192 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions regarding "A Digital Single Market Strategy for Europe" 6/05/2015.

[237] European Commission (2015). COM (2015) 192 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions regarding "A Digital Single Market Strategy for Europe" 6/05/2015.

[238] The Kosciuszko Institute- European CyberSecurity Journal (2015), Volume 1, Issue 1. Strategic Perspectives on Cybersecurity Management and Public Policies

[239] See European Commission (2013). JOIN (2013) 1 final: 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: An Open, Safe and Secure Cyberspace

[240] See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry

[241] See IPOL Study (2015). Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study for the LIBE Committee.

[242] See Accenture and HfS Research (2016). The State of Cybersecurity and Digital Trust 2016.

[243] See European Commission (2016). COM (2016) 410 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Innovative Cybersecurity Industry

[244] See Carrapico, H., Barrinha, A. (2017). The EU as a coherent (cyber)security actor?

[245] See Christou, G. (2014). The EU's Approach to Cyber Security. EUSC EU China Security Cooperation: performance and prospects. Policy paper series. Available at
http://privatewww.essex.ac.uk/~susyd/EUSC/documents/EUSC%20Cyber%20Security%20EU%20Christou.pdf

[246] See interviews

	Data processing and analysis. Difficulties arise to identify consequences and lessons learned once an incident has occurred. This is due to the fact that normalisation of data and processes is problematic, as impacts cannot be measured or identified easily. Thus, comparability becomes arduous. Moreover, testing cannot offer guarantee of success.[247] **Lack of data** is also an issue as a large number of cyber incidents in the EU go unnoticed due to unwillingness to disclose information.[248]

[247] See Bendiek, A. (2012) 'European Cyber Security Policy', SWP Research Paper No13. Available at http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paperdetail/article/european_cyber_security_policy.html Accessed 28 February 2017.

[248] The Kosciuszko Institute- European CyberSecurity Journal (2015), Volume 1, Issue 1. Strategic Perspectives on Cybersecurity Management and Public Policies

European Commission

Evaluation of ENISA
Luxembourg, Publications Office of the European Union

2017 – number pages