Intended for
ENISA

Document type
Final report

Date
May 2016

Framework contract No F-DIR-15-C12

EXTERNAL EVALUATION OF ENISA – 2015 FINAL REPORT

RAMBØLL

EXTERNAL EVALUATION OF ENISA – 2015
FINAL REPORT

Revision	**2**
Date	**27/05/2016**
Made by	**Karin Attström, Vanessa Ludden, Ida Maegaard Nielsen, Franziska Lessmann**
Checked by	**Helene Urth**
Approved by	**Helene Urth**

Ramboll
35, Square de Meeûs
1000 Brussels
Belgium
T +32 02 737 96 80
F +32 02 737 96 99
www.ramboll.com

CONTENTS

TABLE OF FIGURES

TABLE OF FIGURES

APPENDICES

ABSTRACT

ENISA´s objective is to enhance the capability of the European Union, the EU Member States and of the business community to prevent, address and respond to network and information security problems. Building on national and Community efforts, the Agency is a Centre of Expertise in this field. ENISA uses its expertise to stimulate cooperation between actions from the public and private sectors.

The evaluation of ENISA´s activities during 2015 found that ENISA is key in developing a high level of NIS within the EU by fostering information sharing, providing technical expertise, enhancing the awareness of stakeholders to their own preparedness. ENISA has assisted in enhancing the capacity of Member States (most notably smaller Member States) through its activities. The Agency plays an important role in building networks, disseminating good practices and technical studies, and organising training sessions at a technical level.

However, more work needs to be done as cyber security challenges are not being as adequately addressed as they could be by Member States and in the EU. Therefore, the evaluation identifies areas where ENISA can improve its contribution to ensuring a high level of NIS in the EU.

EXECUTIVE SUMMARY

This report presents the findings and conclusions from the **external evaluation of ENISA's core operational activities in 2015**. The **overall objective of the evaluation** was to evaluate the **effectiveness, efficiency, added value, utility, coordination and coherence, and EU added value** of the activities carried out by ENISA, thereby providing ENISA with an evaluation of its performance and an assessment of the possible options for change/improvement.

The scope of the evaluation focussed on ENISA's **core operational activities** in 2015, with an **estimated expenditure above 30,000** Euros. This evaluation is the second in a series of annual evaluations (up until 2018). This year, the evaluation used four main data collection tools/methods, namely: a desk review of relevant documents and data, in-depth interviews with a range of key stakeholders (public and private), an online survey with a broader target group than in the first year, and case studies which focussed on three of ENISA's work packages in 2015. The data quality was judged sufficient to allow for analysis and the development of conclusions.

The table below presents an overview of the **main conclusions and recommendations** of the evaluation in relation to the evaluation criteria.

Conclusion	Recommendation
Relevance	
Ensuring a high level of NIS*:* The evaluation findings confirm that at present cyber security threats are not being adequately addressed in the EU or at the national level in Member States. ENISA´s 2015 core operational activities were shown to be contributing to addressing this gap by supporting the EU and Member States in their efforts to increase NIS. Whether the actual results of activities have met the needs is more difficult to ascertain. Hence it will be important for ENISA to further prioritise its efforts in areas with greatest needs and/or where least attention is being paid to the NIS threats.	It is recommended that ENISA elaborate a framework or methodology for a needs assessment to systematically map and prioritise its work, and act as a guide for the strategic planning of the Agency and the development of Annual Work Programmes. Such a framework would help ENISA and key stakeholders make the "hard choices" and focus efforts where they are most needed. The framework should be discussed and agreed in consultation with key stakeholders.
Supporting differing needs*:* Currently ENISA strikes a balance in how it provides support to Member States depending on their needs and situation. 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 NCSS), while Member States with higher NIS capacity tend to benefit from technical studies, and contribute with best practices.	The Agency should (continue to) be aware of and take into account such differing needs in the work it carries out, e.g. by clustering Member States that have similar needs or objectives. This may seem to contradict the earlier recommendation on prioritisation, but it should be emphasised that prioritisations should be done on the basis of objectives, NIS weaknesses etc. and mot MS or stakeholders.
Effectiveness	
Development of expertise*:* While ENISA is contributing to the development and maintenance of a high level of expertise of EU	ENISA could consider lessening its focus on this more technical objective and invest more resources on a limited number of deliverables

actors, it is doing so to a limited extent. ENISA is considered a "trusted partner" by stakeholders, providing "relevant", "useful", "quality" inputs and advice. However, evidence points to the fact that ENISA's 2015 activities have not led to a significant increase in technical capacity, the promotion of relevant methods towards emerging technologies, or enabled opportunities for new technologies and approaches to a high degree. It is worthy of note that is an ambitious objective for an Agency with limited resources and in many cases it proved too early to judge whether ENISA's 2015 activities have contributed to such a long-term objective.	which provide the most added value / impact. This would make sense considering the expert resources needed to truly add value in this field, Member State's (CSIRT) competence and capabilities in this more operational area, ENISA's more strategic mandate, and ENISA's limited budget. In the future, a needs assessment could be undertaken with key experts to ascertain what the most important needs are.
Building capacity in the EU*:* ENISA managed to enhance capacity building to a significant extent through its 2015 activities, but to varying degrees according to the stakeholder type. ENISA has assisted in enhancing the capacity of Member States (most notably smaller Member States) in particular. However, more work needs to be done as cyber security challenges are not being as adequately addressed as they could be by Member States and in the EU; it is unclear what the role of ENISA is in relation to building the EU institutions' capabilities; and more could be done in relation to the private sector where ENISA remains relatively little known.	In the future, more of a focus could be placed on building capacity within the EU institutions (including the Commission - see recommendation below), as well as increasing awareness of ENISA's work, and thereby further build capacity among private sector actors. The role of ENISA vis à vis the EU institutions could be examined in more detail during the evaluation which is scheduled to take place in 2017.
***Supporting the development and implementation of policy:* In 2015,** ENISA was more effective at supporting the *implementation* than the *development* of the policies necessary to meet the legal and regulatory requirements of NIS. ENISA's key contribution to the *implementation* of policies related to NIS resides in its thorough understanding of the legal basis, the technical context, and stakeholders' views, however it plays a lesser role in the *development* of policies.	Though potentially difficult due to resource constraints and the Commission and Member States' perceptions of ENISA's supportive (rather than central) role in the development of policies related to NIS, it may be beneficial to involve the Agency in the development of policies related to NIS through more coordination with the Commission and Member States. This would allow ENISA to ensure a consistent approach to cyber security across the various sectors concerned by given policy/legislative developments.
Impact	
Ensuring a high-level of NIS*:* The evaluation found that ENISA makes an important contribution to ensuring a high level of NIS in the EU, but also indicates that more could be done in terms of further engaging with the institutions at EU level and focusing on tangible outputs like incident reporting.	It is recommended that the Agency focus on the areas which deliver the highest impact. These areas are suggested to be: providing expertise on specific technologies, including methodologies on how to assess the technologies advantages/disadvantages; events (in particular the Annual Privacy Forum - APF); and exercises (in particular the Cyber Europe exercise) where stakeholders network and learn from each other.

Raising awareness of NIS: The evaluation found that awareness raising on NIS is considered essential by most stakeholders and the role of ENISA in this regard was assessed as pivotal. The findings indicated that some improvements could be made.	In order to further increase its impact on awareness raising, it is recommended that ENISA: • Improve its collaboration with NLOs, in particular by clarifying their role and scoping their tasks. • Continue implementation of its awareness raising capacity. • Improve effective dissemination of publications (through NLOs, its website, social media - in particular LinkedIn which appears to be used by different categories of stakeholders).
Achievement of impact: For ENISA, measuring impact is highly challenging and to a large extent dependent on contextual factors. Moreover, impact can often only really be judged on the longer term through an annual monitoring process. In this respect, ENISA´s annual Key Impact Indicators (KIIs) are an essential data source when it comes to monitoring the Agency´s impact over time. However, 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.	It is 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. 5 years. It is 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.
Efficiency	
Organisational set-up and processes: ENISA generally functions efficiently; it is characterised by a clear delineation of responsibilities and has cost-saving measures in place, but one case of low efficiency was identified, namely the insufficient dissemination of publications.	By boosting its dissemination of publications, ENISA would be increasing its cost-effectiveness, since more stakeholders could benefit from the publications. As shown above, improved efforts from the NLO network could be one tenant in achieving this at a reasonable cost.
Coordination and coherence	
Good coordination with other stakeholders*:* The evaluation shows that ENISA coordinates activities with relevant bodies, offices and agencies in the field of Information and Communications Technologies (ICT), though more could be done to align activities with other stakeholders in industry, academia and FRA, while keeping in mind that this remains an area of MS competence.	It is recommended that ENISA increase its coordination with private sector stakeholders, as well as increase their involvement in its activities (for example Future Cyber Security Private-Public Partnerships). Amongst EU bodies, ENISA´s expertise is largely unique, and its technical advice has potential to make an important contribution to other EU bodies, such as FRA, as was seen

	when cooperation between the two agencies was explored during 2015. Other examples include Europol and EU-LISA.
EU added value	
Duplication of efforts*:* It is assessed that there were cases where ENISA´s 2015 activities duplicated the efforts of national and EU level stakeholders, and where the information provided by the Agency is provided by other sources. Such instances will reduce efficiency, and limit ENISA´s effectiveness. At the same time, it should be noted that ENISA's 's 2015 activities have EU added value, because the Agency has a strong role in capacity building and advocating information security at EU level, and supports Member States in implementing EU policies. Moreover, ENISA provides unique technical expertise at an EU level.	A more careful examination of cases where ENISA´s work overlaps or duplicates the work of other EU or national level stakeholders should be undertaken to ascertain when and with which organisations overlap occurs; how a duplication of efforts can be avoided; and which justifications there may be for multiple sources providing the same information (e.g. complementary information, ensuring an independent source of information, providing timely information or similar).

1. INTRODUCTION

This final report presents the findings and conclusions from the external evaluation of ENISA's core operational activities in 2015. The overall objective of the evaluation was to evaluate the effectiveness, efficiency, added value, utility, coordination and coherence of the activities carried out by ENISA, thereby providing ENISA with an evaluation of its performance and an assessment of the possible options for change/improvement.

The legal basis for the evaluation includes:

- The Financial Regulation applicable to ENISA, whereby Article 29 (5) stipulates that ex–post evaluations shall be undertaken and that such evaluations shall be undertaken for all programmes and activities which entail significant spending. The results of such an evaluation are to be sent to the Management Board.
- Article 11.2(f) of the ENISA Regulation (EU) No 526/2013 which stipulates that the Executive Director shall be responsible for preparing the action plan following-up on the conclusions of the retrospective evaluations and reporting on progress every two years to the Commission.

The scope of the evaluation was defined in the terms of reference as ENISA's core operational activities (in 2014) with an estimated expenditure exceeding EUR 30,000.

It was foreseen that the evaluation of ENISA's activities should serve three purposes:

1. Provide reliable performance information to assist management to deliver against targeted results, to address problems promptly and to take planning and budget decisions;
2. Improve learning through regular review of ENISA activities improving internal functioning and providing staff and stakeholders with opportunities to learn more about the effectiveness and performance of the Agency;
3. Strengthen accountability and transparency providing empirical evidence on the outcomes of ENISA's activities and thus provide reliable information on results to the EU institutions, Member States, and relevant stakeholders and to the public.

This evaluation is the second in a series of annual evaluations (up until 2018). Details of the methodology employed, including strengths and weaknesses of the chosen approach, are presented in chapter 3. This year, the evaluation used four main data collection tools/methods, namely: a desk review of relevant documents and data, in-depth interviews with a range of stakeholders, an online survey with a broader target group than in the first year, and case studies which focussed on three of ENISA's work packages in 2015. In subsequent years, the methodology will be further refined and adapted, while still enabling the tracking of performance.

This draft report contains the following sections:
Chapter 2: Policy context and background of ENISA
Chapter 3: Methodology (detailed evaluation matrix in Appendix 1 and M&E framework in Appendix 3)
Chapter 4: Findings of the evaluation
Chapter 5: Conclusions and recommendations
Chapter 6: Action plan

A score board of achievements, the complete survey results, an analysis of publication downloads for 2014 and revised evaluation forms can be found in the appendices, while the case study reports for Work Packages 1.2, 2.1 and 3.3 can be found in separate annexes sent along with this report.

2. POLICY CONTEXT

This chapter presents the context of the evaluation and highlights the rationale for the establishment of the European Union Agency for Network and Information Security (hereinafter: ENISA or the Agency), as well as its political context, and how this has gradually changed. Additionally, the chapter presents the legal background, mission and activities of the Agency and outlines its most important stakeholders.

2.1 EU´s role in developing Network and Information Security

Communication networks and information systems have become an essential factor in economic and societal development. Their security and, in particular their availability, is of increasing concern to society because of the possibility to encounter problems in key information systems, due to system complexity, accidents, mistakes or attacks which may have consequences for the physical infrastructures which deliver services critical to the well-being of EU citizens. Moreover, the growing number of security breaches has already generated substantial financial damage and undermined user confidence. At the same time, the Information Society is becoming indispensable in all areas of life and the modernised Information Society of Europe and its business, based upon a Digital Economy is thus, potentially, jeopardised.

Network and Information Security (NIS) has been on the agenda for EU policy makers since the 2001 Communication of the European Commission on NIS[1]. In that same year, the Framework Decision on combating fraud and counterfeiting was adopted[2], which defined the fraudulent behaviours that EU States need to consider as punishable criminal offences. The following year – the ePrivacy Directive[3] was adopted, binding providers of electronic communications services to ensure the security of their services and maintain the confidentiality of client information.

In 2013, the European Commission proposed a Directive on Network and Information Security which is currently in the final stages of negotiations between the European Parliament and the Council. The Directive has as core aims: (a) improving Member States' national cybersecurity capabilities, (b) improving cooperation between Member States and public and private sectors, (c) requiring companies in critical sectors to adopt risk management practices and report major incidents to the national authorities. It is envisaged that the implementation of the Directive will bring more trust to citizens and consumers in technologies, the increase in usage of digital networks by governments and businesses and the Directive will boost the EU economy creating more equal and stable conditions on the Digital Single Market. As it stands currently, the proposal ensures a pivotal role for ENISA in advancing the EU Member States agenda on NIS. Furthermore, the proposal also reinforces the role of Member States in the NIS agenda envisaging the establishment at national level of NIS Strategies defining strategic objectives and appropriate policy of networks and information systems.[4]

Recently, on 4th of May 2016, the EU adopted the General Data Protection Regulation (GDPR)[5] and the Directive on data protection[6], which have been published in the EU Official Journal. The Regulation will enter into force on 24 of May 2016 and it shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018. The EU Data Protection legislative reform is anticipated to

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

[2] 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment

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

[4] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 15229/2/15 REV 2, 6342/13 TELECOM 24 DATAPROTECT 14 CYBER 2 MI 104 CODEC 313, Brussels 18.12.2015

[5] 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)

[6] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market.

2.2 Establishment of ENISA

ENISA was established in 2004 by the European Parliament and the Council of the European Union in response to a growing number of security breaches, generating substantial financial damage, undermining user confidence and slowing down the development of e-commerce. At a time when individuals, public administrations and businesses reacted to these developments by deploying security technologies and security management procedures and Member States took several supporting measures, the EU also felt the necessity to help minimise risks to ensure the smooth functioning of the Internal Market. It did so by creating an agency to tackle challenges related to NIS, which encompasses both cyber security and Critical Information Infrastructure Protection (CIIP).

ENISA was tasked[7] with contributing to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union. In 2006, the European Commission aimed to give new momentum to European NIS by developing a strategy for a secure information society and giving ENISA an essential role as a centre promoting information sharing, cooperation amongst all stakeholders, and the exchange of commendable practices. The approach was based on a dialogue to bring together all stakeholders and empower them through dialogue[8].

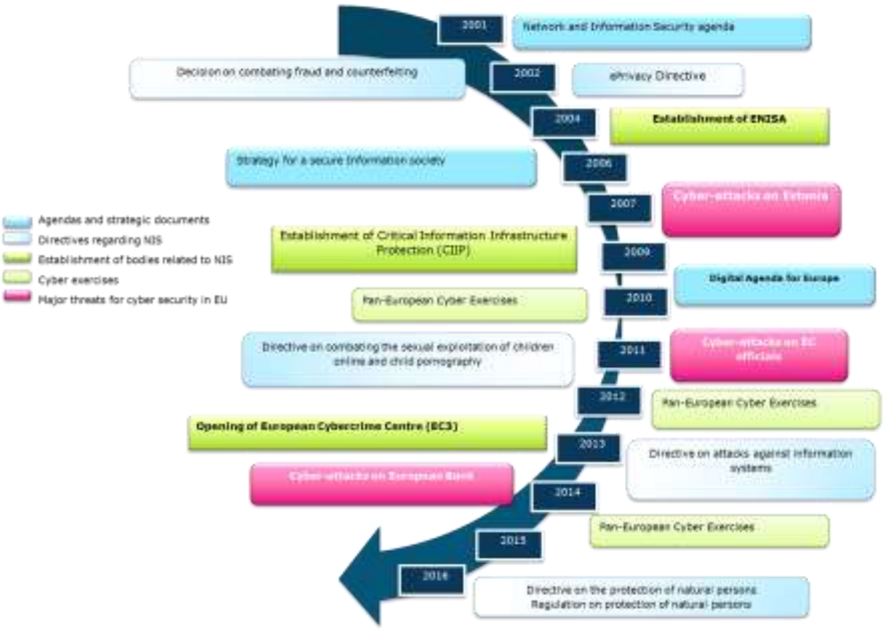
After the large-scale cyber-attacks on Estonia in 2007, an EU initiative on CIIP was established in 2009[9]. The 2010 Digital Agenda for Europe stressed the importance of trust and security and highlighted the pressing need for all stakeholders to join forces and develop effective and coordinated mechanisms to respond to new and increasingly sophisticated cyber risks. The figure below shows the timeline of key developments and milestones in NIS at the European level.

[7] Regulation 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency

[8] COM(2006)251, A strategy for a secure Information society – dialogue, partnership and empowerment

[9] Communication on Critical Information Infrastructure Protection – Protecting Europe form large scale cyber-attacks and cyber-disruptions : enhancing preparedness, security and resilience, COM (2009) 149

Figure 1 Timeline of key developments in NIS in Europe


2001
Network and Information Security agenda
Decision on combating fraud and counterfeiting
2002
ePrivacy Directive
2004
Establishment of ENISA
Strategy for a secure information society
2006
Agendas and strategic documents
Directives regarding NIS
Establishment of bodies related to NIS
Cyber exercises
Major threats for cyber security in EU
2007
Cyber-attacks on Estonia
Establishment of Critical Information Infrastructure Protection (CIIP)
2009
Digital Agenda for Europe
Pan-European Cyber Exercises
2010
Directive on combating the sexual exploitation of children online and child pornography
2011
Cyber-attacks on EC officials
2012
Pan-European Cyber Exercises
Opening of European Cybercrime Centre (EC3)
2013
Directive on attacks against information systems
Cyber-attacks on European Bank
2014
Pan-European Cyber Exercises
2015
2016
Directive on the protection of natural persons
Regulation on protection of natural persons

Source: Ramboll Management Consulting based on ENISA and EC websites

The most recent EU legislative actions contributing to the fight against cybercrime include the 2011 Directive on combating the sexual exploitation of children online and child pornography[10], which better addresses new developments in the online environment and the Directive on attacks against information systems[11] in 2013, which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions. Additionally, the European Commission has played a key role in the development of European Cybercrime Centre (EC3)[12], which started operations in January 2013. EC3 acts as the focal point in the fight against cybercrime in the Union, pooling European cybercrime expertise to support Member States' cybercrime investigations and providing a collective voice of European cybercrime investigators across law enforcement and the judiciary.

Finally, 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[13]. The DAE's main objective is to develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe. The 3rd pillar of the DAE is specifically addressing Trust & Security issues[14] and serves as an umbrella for all EU conducted and coordinated activities in the field of NIS.

[10] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA

[11] Directive 2013/40/Eu Of The European Parliament And Of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

[12] Europol, The European Cybercrime Centre (EC3) – First Year Report, 2014 < https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report>

[13] COM (2010) 2020 final, Communication from the Commission Europe 2020, A strategy for smart, sustainable and inclusive growth; Brussels, 3.3.2010

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

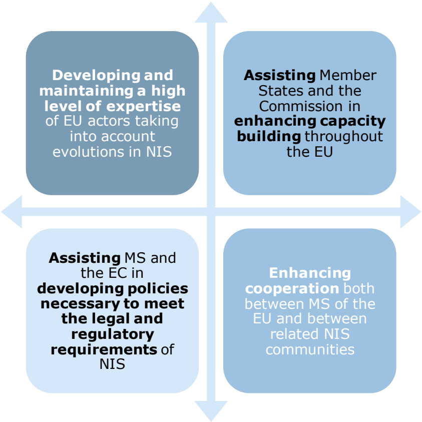
2.3 Legal background and mission

ENISA's legal basis can be found in Regulation (EC) No 460/2004[15], which established the Agency, two later extensions of ENISA's mandate, i.e. Regulation (EC) No 1007/2008[16] and Regulation (EC) No 580/2011[17], and, finally, the new ENISA basic Regulation (EU) No 526/2013[18] of the European Parliament and of the Council, adopted in 2013 and repealing Regulation (EC) No 460/2004. The regulation outlines the objectives and tasks of ENISA, and also outlines the governance structure, with a Management Board and a Permanent Stakeholders Group.

2.3.1 ENISA's objectives

In light of the previously described context of intensifying cyber threats, the Agency's objectives is to enhance the capability of the European Union, the EU Member States and of the business community to prevent, address and respond to network and information security problems. Building on national and Community efforts, the Agency is a Centre of Expertise in this field. ENISA uses its expertise to stimulate cooperation between actions from the public and private sectors. ENISA's specific objectives are presented in the figure below[19].

Figure 2 Specific objectives of ENISA



Developing and maintaining a high level of expertise of EU actors taking into account evolutions in NIS

Assisting Member States and the Commission in **enhancing capacity building** throughout the EU

Assisting MS and the EC in **developing policies necessary to meet the legal and regulatory requirements** of NIS

Enhancing cooperation both between MS of the EU and between related NIS communities

Among other things, the Agency provides assistance to the European Commission and Member States in their dialogue with the industry to address security-related problems in hardware and software products. ENISA also follows the development of standards, promotes risk assessment activities conducted by Member States and interoperable risk management routines, and produces studies on these issues within public and private sector organisations.

The Agency works closely together with members of both the public and private sector to deliver advice and solutions that are based on solid operational experience. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, Computer Emergency Response Team (CERT) cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat

[15] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)
[16] Regulation (EC) No 1007/2008 Of The European Parliament And Of The Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration
[17] Regulation (EC) No 580/2011 Of The European Parliament And Of The Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration
[18] 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
[19] Objectives as agreed with the ENISA Management Board in the annual work programme 2014

landscape. ENISA also supports the development of the EU policy and law on matters relating to NIS, thereby contributing to economic growth in Europe's internal market.

2.4 ENISA's tasks and activities

The Agency's tasks, as per the establishing Regulation, focus on:

- ✓ Advising and assisting the European 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.
- ✓ Awareness-raising and 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 NIS Good Practice Brokerage activities, which are based on the concept of the exchange of good practices between EU Member States in the area of NIS on a pan-European scale.

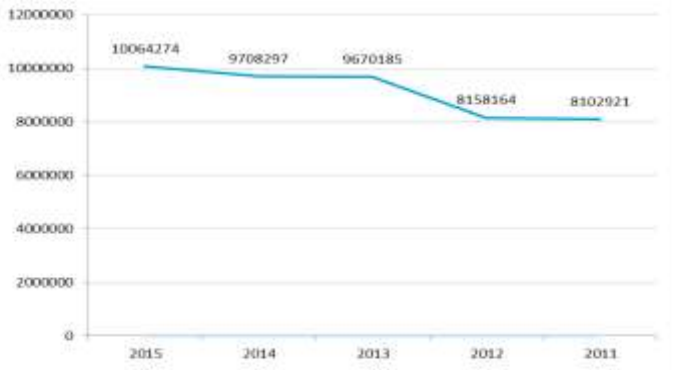
2.5 ENISA's organisation and resources

As provided in the ENISA Regulation (EU) No 526/2013, the bodies of the Agency consist of:

- ✓ Management Board: tasked to ensure that the Agency carries out its tasks under conditions which enable it to serve in accordance with the founding Regulation.
- ✓ Executive Board: responsible for preparing decisions to be adopted by the Management Board on of administrative and budgetary matters
- ✓ Executive Director: responsible for managing the Agency and performing his/her duties independently.
- ✓ Permanent Stakeholders' Group (PSG): who advises the Executive Director in the performance of his/her duties under this Regulation.
- ✓ Ad hoc Working Groups: the Executive Director establishes, in consultation with the PSG, ad hoc Working Groups composed of experts. The ad hoc Working Groups are addressing specific technical and scientific matters.

In terms of budget execution, the expenditure appropriations of ENISA Budget 2015 of 10.064.274 €, were committed at a rate of 100% on 31/12/2015. The figure below presents the budget of ENISA per year from 2011 to 2015.

Figure 3: Budget of ENISA (2011-2015)



Source: Annual Budget, 2011-2015

In terms of staff, at the end of 2015, 69 statutory staff were employed in the Agency. During 2015, four staff left the Agency, seven vacancy notices were published and seventeen staff were recruited or took up new duties within the Agency. As reported in the Annual Activity Report, ENISA still experiences significant challenges in attracting and holding suitably qualified staff to support the activities of the Agency. The changes in terms of staff constitute a challenge due to several factors, mainly the types of post that are being offered (CA posts) and the low coefficient factor which applies to salaries of ENISA employees in Greece.[20]

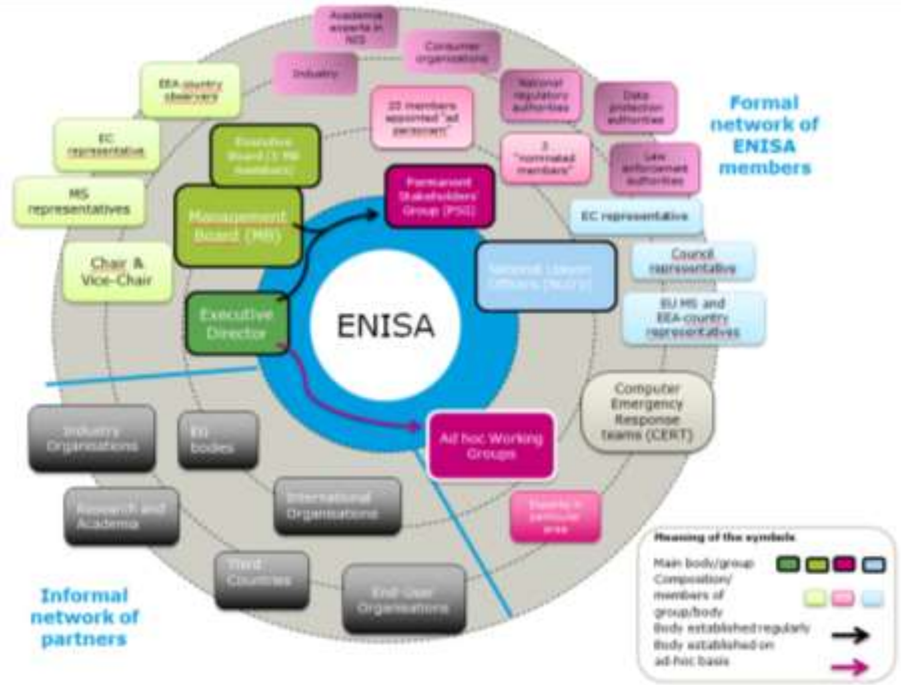
2.6 ENISA's stakeholders

ENISA's stakeholder relations are a key factor in the success of its 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. In addition to the formal organisational bodies established by EU regulations, ENISA set up and maintains a formal group of liaison officers, called **The Network of Liaison Officers** (NLOs or the "local community"). Although not formally based on the ENISA Regulation, this network is of value to ENISA as the NLOs serve as ENISA's key point 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 it 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 Management Board (MB) 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, e.g.).

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. The open and growing network of stakeholders is essential to the Agency's goals in identifying emerging risks and forging new insights into helping Member States and private sector organisations through access to NIS experts. Figure 4 shows a map of ENISA's stakeholders who are vital and essential partners to its activities.

[20] ENISA, 2015: Annual Activity Report, pp. 45ff.

Figure 4 ENISA's stakeholder map


Academia experts in NIS
Consumer organisations
Industry
EEA country observers
EC representative
MS representatives
Chair & Vice-Chair
Executive Board (3 MB members)
Management Board (MB)
Executive Director
20 members appointed "ad personam"
Permanent Stakeholders' Group (PSG)
National regulatory authorities
Data protection authorities
3 "nominated members"
Law enforcement authorities
Formal network of ENISA members
EC representative
National Liaison Officers (NLO's)
Council representative
EU MS and EEA country representatives
ENISA
Computer Emergency Response teams (CERT)
Ad hoc Working Groups
Experts in particular area
Industry Organisations
EU bodies
Research and Academia
International Organisations
Third Countries
End-User Organisations
Informal network of partners
Meaning of the symbols
Main body/group
Composition/ members of group/body
Body established regularly
Body established on ad-hoc basis

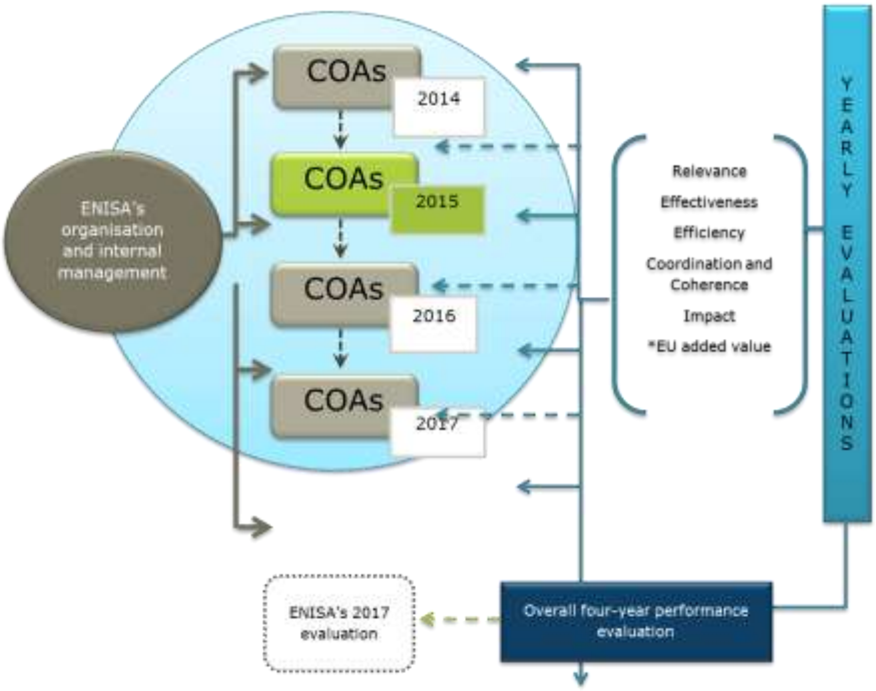
Source: ENISA website, *Structure and Organisation, Stakeholders Relations*

3. METHODOLOGY

3.1 Evaluation framework

The current external evaluation forms part of a framework contract which enables yearly evaluations of ENISA from 2014 to 2017. The framework developed for the first year's evaluation (2014) has been designed to ensure that it can be applied in subsequent years, in order to generate robust findings over time. This is illustrated by the figure below, which presents our overall approach to the assignment.

Figure 5: Our approach to the evaluation of ENISA's core operational activities



In order to meet the requirements, we have developed a two tier evaluation framework, one overall framework to be applied to all the years being evaluated (evaluation questions matrix[21]) and one more detailed Monitoring and Evaluation (M&E) framework looking to assess the effectiveness of the core operational activities for each year (2015 in this instance). The evaluation questions matrix contains questions relating to the evaluation criteria listed in the figure above (e.g. effectiveness, relevance, etc.). The M&E framework has been developed on the basis of the intended outcomes and results of ENISA's strategic objectives, as presented in the intervention logics included in Appendix 2.

As agreed at the kick off meeting for the 2015 evaluation, the EQ Matrix has been extended to also assess the EU added value of ENISA. This is a key evaluative criterion of the Commission's

[21] An evaluation questions (EQ) matrix is a tool used to structure an evaluation by specifying the questions to be addressed, indicators to be used, judgement criteria and data sources. In this way, a EQ matrix serves to ensure that findings are solid, robust and transparent.

Better Regulation guidelines. The assessment will build on the terms of the study which specify the need to assess the added value of the core operational activities, and ensure that a sufficient focus is put on the added benefits of approaching NIS at EU level, including the principles of subsidiarity and proportionality.

The evaluation matrices can be found in Appendix 1 and Appendix 3, including a score board assessing the 2015 results against the set targets.

3.2 Sources and data collection

The evaluation findings have been generated using different types of data sources, as illustrated in the evaluation matrices. The primary sources are listed in the table below.

Table 1 Data collection and sources

Data collection	Source
Desk review	• Work Programme 2015 • Annual Report 2015 (draft) • Regulation (EU) No 526/2013 • Financial data from ENISA • Web statistics from ENISA
Interviews	• In-depth interviews with: • 2 MEPs[22] • 2 Commission officials • 2 representatives of the PSG • 5 members of the Management Board
On-line survey	• On-line questionnaire to Management Board (MB) members and National Liaison Officers (NLOs), Permanent Stakeholder Group (PSG) industry representatives, the European Commission and other selected stakeholders
Case studies on WPK 1.2, 2.1 and 3.3	• Review of Work Programme 2015 and Annual Report 2015 (draft) • Interviews with 2 NLOs • Interviews with up to 4 targets of the WPKs concerned[23] • Web statistics from ENISA

Data collection was carried out from early March to mid-May 2016. The process worked well overall, though it proved difficult to both identify and interview the number of people that we aimed to interview as part of the case studies. Multiple efforts were made to identify relevant interviewees per WPK, including enabling survey respondents to register their interest for taking part in an interview, using participant lists of given events and training sessions, identifying expert contributors to given publications, and (where these efforts did not bear fruit) asking ENISA to provide the details of relevant "targets". The support provided by ENISA to the evaluation exercise was highly valuable and essential to reaching relevant stakeholders.

A **survey** was conducted with key stakeholders. The questionnaire was based on the evaluation framework developed, and included questions relating to the outcomes, results and impacts of ENISA's strategic objectives in 2015. Due to concerns about the confidential nature of the contact details of those targeted by the survey, all of those surveyed received a link via an e-mail sent by ENISA. Considering a decision was taken to target a wider population of stakeholders this year relative to last year, the response rate was relatively low, despite a follow-up having been sent a week before the survey was closed. That said, a broad range of stakeholders is represented, as Table 2 below illustrates and 100 stakeholders have been included in the survey analysis (compared to 63 in 2014).

The survey questionnaire was developed on the basis of last year´s survey, and is thus based on the evaluation questions matrix and the Monitoring and Evaluation (M&E) framework for

[22] Significant efforts were made to speak to another 2 MEPs in order to achieve the intended target number of interviewees, but these interviews were declined.

[23] A total of 31 "targets" of these WPKs were contacted (including follow-ups by email and/or phone) and multiple approaches used to identify relevant interviewees over the course of the data collection period, but unfortunately we were not able to interview the 5 "targets" we were aiming for per case study. In the case of WPK 1.2, 4 "targets" were interviewed, 4 for WPK 2.1 and 4 for WPK 3.3.

deliverables developed as part of the initial phase of this evaluation (see inception report of the ENISA evaluation 2015). One key change to the survey was the addition of the brief targeted survey which was added to the end of the survey to further investigate respondents' use of specific deliverables under the 2015 COAs.

The survey was sent out via e-mail by ENISA to 748 persons, and was open from March 23th 2016 until April 12th 2016. To encourage responses, a follow-up email was sent to respondents on April 5th 2016.

Table 2 Overview of the distribution of the survey

Respondent category	No. of persons
Management Board	77
Permanent Stakeholder Group	25
National Liaison Officers	20
Industry	67
CERT Network	44
CRM contacts	250
NCSS Expert Group	33
NCSS stakeholders	81
Group on cloud security	44
Group on eHealth Sec	20
Group on SCADA EICS	24
Group on SCADA EUROSCSIE	35
Group on Finance	28
Total	**748**

The survey was completed by 86 respondents, and an additional 38 respondents partially completed the survey. The partially completed responses are those where responses have not clicked "submit survey" at the end or where they did not finish the survey[24]. The partial responses to the survey were examined in detail, and several of them were answered to a high extent. In other to preserve the integrity of the analysis, while not excluding valuable data, partially completed surveys were included in the analysis. The selection criterion for including these responses was whether a response included a completed section of the survey questions, for example, all questions related to "Relevance of ENISA's work".

Table 3 Responses included in the survey

	No. respondents who opened the survey	No. of respondents who partially completed the survey	No. of respondents who completed the survey
Total	210	38	86
Included in the survey	100	14	86

The total pool of respondents thereby includes 100 persons, giving a response rate of 13.4%. This is a low response rate, which is in part explained by the fact that a large group of stakeholders were contacted, that there may have been duplicate emails (meaning that one respondent is counted more than once) and that many stakeholders filled in the survey last year – leading to survey fatigue. Since the response rate amongst respondents who opened the survey is high at nearly 50%, the main reasons for the low responses are likely connected with external factors, rather than to do with the survey design itself.

Aside from the respondents who completed or partially completed the survey, 86 persons opened the survey by clicking on the link that was distributed, but did not respond to any questions. This means that a total of 538 persons who received the survey did not click on the link at all.

[24] Since the survey was implemented with an emphasis on anonymity, as agreed with ENISA, it was not possible for respondents to save their survey responses (as stated in the introduction to the survey), which may have prevented some respondents from completing the survey.

All respondent categories are represented in the survey, ensuring satisfactory coverage[25]. In total respondents from all Member States except Slovakia are included in the survey.

The data quality is judged sufficient to allow for analysis and the development of conclusions; we have interpreted the data with due consideration, and taken the response rate into account throughout the analysis. Throughout the analysis of survey findings, the agreed threshold or judgement norm of 70% agreement is consistently being used to assess performance. Survey responses can be found in Appendix 5.

The **case studies** this year focus on given work packages (WPK) and the Core Operational activities (COAs) within these, and are distributed across the four Strategic Objectives (SOs) for 2015 (as set out in ENISA´s annual work programme). Since last year´s evaluation conducted a case study on the cyber exercise, which falls under Strategic Objective 4 (SO4), this year´s evaluation focussed on WPKs carried out under the remaining three SOs, namely:

- SO1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)
- SO2: To assist the Member States and the Commission in enhancing capacity building throughout the EU
- SO3: To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security

The selected SOs are also allocated the highest budget volume. Within the three SOs, we covered the WPKs with the highest budget allocations, as presented in the table below.

Table 4 Overview over the case study selection

Strategic Objective (SO)	Work package (WPK)	Deliverables[26]
SO1	1.2	D1 - Stock Taking, Analysis and Recommendations on the protection of CIIs D2 - Methodology for the identification of Critical Communication Networks, Links, and Components D4 - Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector D5 - Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services
SO2	2.1	D1 - Support and Advise Member States on the establishment and evaluation of National Cyber Security Strategies (NCSS) D3 - Maintaining CERT good practice and training library D4 - Building upon the evaluation update ENISA’s methods in CERT capacity building and propose a roadmap D5 - Impact evaluation on the usefulness of the ENISA guidelines on capacity building
SO3	3.3	D1 - Readiness analysis for the adoption and evolution of privacy enhancing technologies D4 - State-of-the-art analysis of data protection in big data architectures

[25] Unfortunately, only one MEP (European Parliament) replied to the survey, limiting the explanatory power of the survey analysis for this group of stakeholders. This means that the MEPs response will be referred to keeping this in mind, i.e. that it does not represent a group of stakeholders.

[26] The identified deliverables are above €30,000 according to the excel file (Table 3 – Budget implementation 2015) sent to the evaluator by ENISA on February 2nd 2016.

These case studies are reported in separate case reports, sent along with this report, and their findings/conclusions have been integrated into relevant parts of the analysis presented below.

In order to ensure that **ENISA´s evaluation forms** focus more on outcomes relative to organisational aspects, we redesigned them and developed an additional follow-up form. The redesign draws both on our experience with designing such forms in general, as well as specific experience with collecting data to evaluate and assess ENISA´s activities. The principles and reasoning behind this task, as well as the proposed forms, are included in Appendix 9.

As part of this year's evaluation, we took a more in-depth look at the **download rates** of ENISA's 2014 publications above the value of €30,000 in order to develop a firmer baseline for the future evaluations than was included in the evaluation of ENISA conducted in 2014 (presented in the final report). It was not possible to conduct a similar analysis of the publications from 2015, since some of these only came online recently (in 2016), which would not give an accurate picture of the downloads of these publications; they will be analysed in next year's evaluation. The analysis is presented in Appendix 6, an update of the assessment of the efficiency of ENISA's 2014 publications on the basis of this revised data is presented in Appendix 7, and summaries of the compiled data are included in Appendix 8.

Due to the very nature of ENISA's work as a knowledge broker and facilitator, much of the findings relate to the perception and opinion of stakeholders on whether ENISA's support has contributed to reaching objectives in NIS and cyber security. In comparison to last year, a larger sample and broader range of stakeholders was targeted, thereby generating more robust conclusions on the achievements of ENISA, though attempts should be made in the future evaluations to increase the buy-in of stakeholders into the evaluation process and cast the next even wider.

4. FINDINGS OF THE EVALUATION

4.1 Overall assessment of the relevance of ENISA´s activities

The assessment of relevance is based on stakeholder's opinions of whether activities are responding to needs and expectations in the EU and Member States, and on the extent to which the actual outputs have been useful (utility).

Conclusion on relevance

Based on the findings, it can be concluded that ENISA´s 2015 activities clearly responded to a need in the European NIS landscape. The survey findings point to the fact that cyber security challenges are not adequately addressed in the EU and Member States, suggesting that much remains to be done to ensure NIS and cyber security. The case studies point to the fact that ENISA's stakeholders' needs differ, with some results being more relevant to given types of stakeholders than others (for example because they corresponded to priorities in Member States). Despite these differing needs, the scope and objectives of ENISA's work during 2015 are seen as relevant to responding to the needs, and ENISA's work and outputs are judged to be responding to a need for NIS across the EU and within Member States. ENISA was further judged to be effectively meeting its stakeholders' expectations.

However, at the same time, stakeholders see limits in ENISA's mandate and outreach, which affects the ability of the Agency to effectively meet the needs in general. Moreover, the survey findings suggest that it is not clear what ENISA expects from its stakeholders, which seems to indicate that there is potential for improving communication with stakeholders.

Comparable findings and a similar conclusion was drawn in last year's evaluation which focussed on the 2014 core operational activities and asked the same questions.

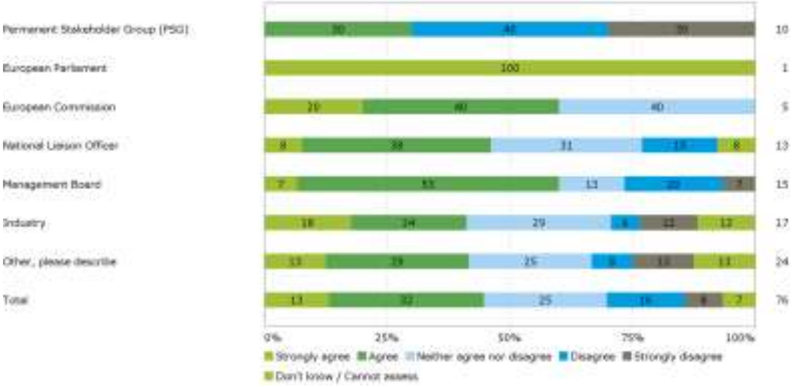
Detailed findings per data source are presented below.

Survey findings

The survey findings suggest that there is a need for NIS in Europe and the vast majority of stakeholders perceive that the scope and objectives of ENISA's work, as well as its outputs, responds to the needs for NIS.

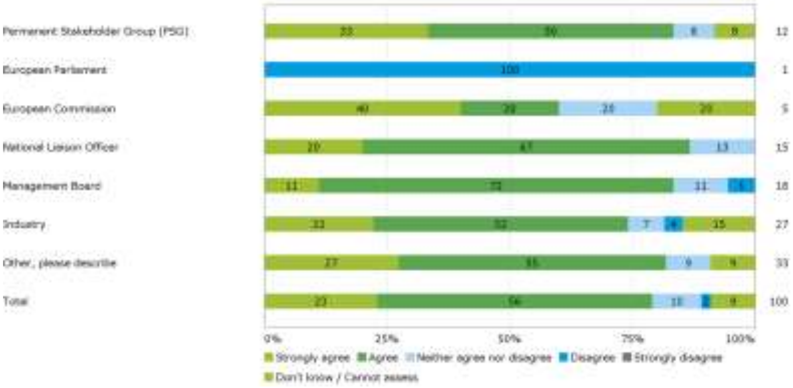
In the survey, stakeholders were asked if cyber security challenges are adequately addressed in the EU. It is clear from responses that a majority of respondents were either neutral or negative, with the Management Board and European Commission being somewhat more positive, as illustrated in Figure 6 below. A similar question looking at whether cyber security challenges are adequately addressed at the Member State level revealed that 41% (strongly) agreed and 24% disagreed (completely) with the statement (survey Appendix 5). Based on these responses, it can be concluded that stakeholders perceive that much remains to be done to ensure NIS and cyber security.

Figure 6: Q3.8 Cyber security challenges are adequately addressed in the EU



A combined 81%[27] of respondents to the survey (clearly above the threshold of 70% agreeing[28]), indicate that the work of ENISA is relevant to responding to the need for NIS in the EU and across Member States, as the figures below further illustrate. This is a strong finding in light of the stated need to ensure NIS and cyber security, as indicated previously.

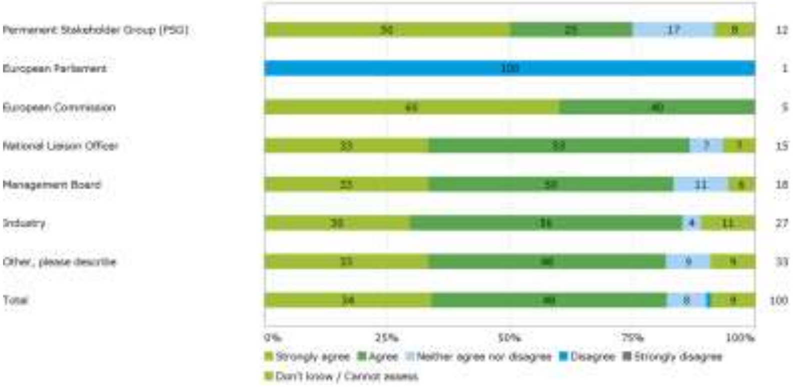
Figure 7: Q1.1 Relevance of the scope and objectives of ENISA's work to responding to the needs for NIS in the Member States



[27] Taken from Survey Question 1.1 and 1.2

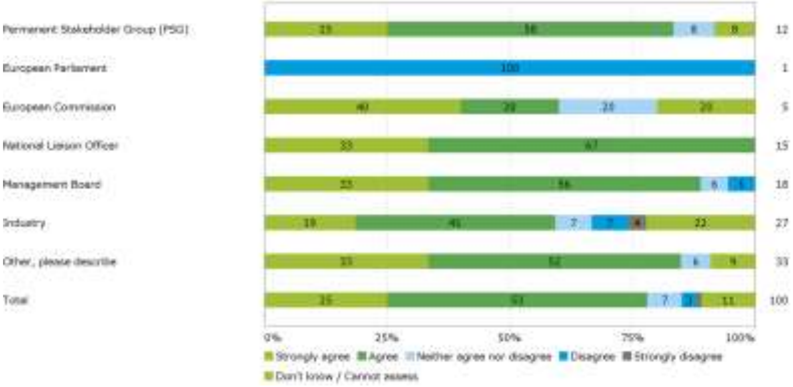
[28] The threshold/judgement criteria defined in the evaluation framework.

Figure 8: Q 1.2 Relevance of the scope and objectives of ENISA's work to responding to the needs for NIS in the EU



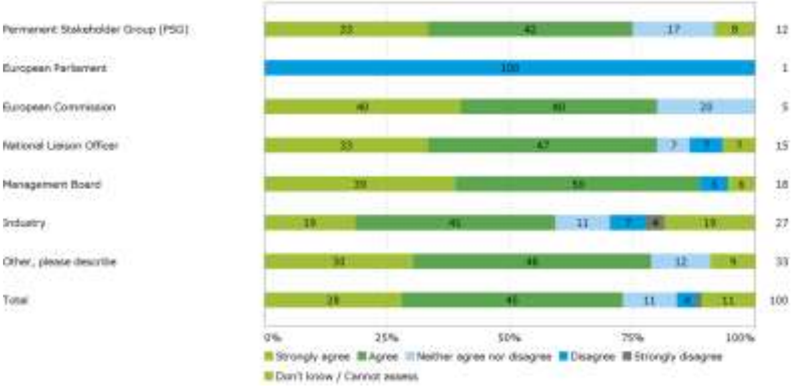
Moreover, a total of 76%[29] of survey respondents agree that ENISA's outputs are responding to the needs for NIS across Member States and in the EU, as the figures below further demonstrate.

Figure 9: Q 1.3 The outputs produced by ENISA are responding to the needs for NIS in the Member States



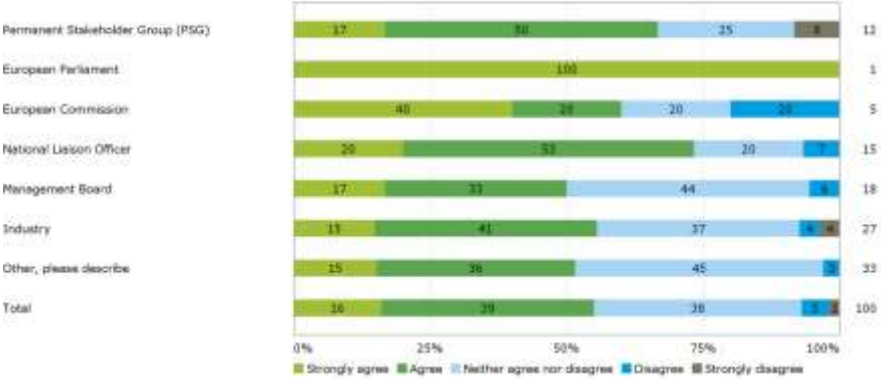
[29] Survey Question 1.3 and 1.4 combined

Figure 10: Q 1.4 The outputs produced by ENISA are responding to the needs for NIS in the EU



Further adding to this positive perception of ENISA and the work it does, 75% of respondents confirm that ENISA is effectively meeting its stakeholders' expectations[30]; see Appendix 5 for the detailed findings. There are, however, areas in which ENISA can still improve. Only 55% of survey respondents state that it is clear what ENISA expects from its stakeholders.[31] This seems to indicate that there is potential for improving communication with stakeholders.

Figure 11: Q 1.7 It is clear what ENISA expects from stakeholders



Additional comments provided by those surveyed suggest that the scope of the mandate of ENISA is currently limiting the possibility for ENISA to further increase its relevance. This, in part, explains the challenge of ENISA in managing stakeholder expectations: The work of ENISA might be relevant outside the direct scope of its mandate, but the possibilities to act upon this are limited.

Case studies

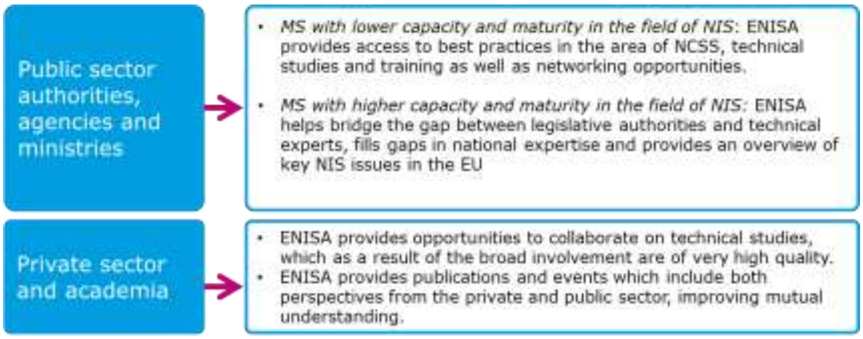
Overall, the case studies confirmed that ENISA´s activities in 2015 were generally relevant to both the public and private sector on national level, in particular since ENISA is an important neutral source of information, in a field where many reports would be written, for example, by providers themselves wanting to sell their own solutions. The case studies showed that the needs

[30] Survey Question 1.6

[31] Survey Question 1.7

of the stakeholders differ, and an in-depth analysis suggests that ENISA addresses different needs.

Figure 12: ENISA´s relevance to the public and private sector



Public sector authorities, agencies and ministries

- *MS with lower capacity and maturity in the field of NIS*: ENISA provides access to best practices in the area of NCSS, technical studies and training as well as networking opportunities.
- *MS with higher capacity and maturity in the field of NIS:* ENISA helps bridge the gap between legislative authorities and technical experts, fills gaps in national expertise and provides an overview of key NIS issues in the EU

Private sector and academia

- ENISA provides opportunities to collaborate on technical studies, which as a result of the broad involvement are of very high quality.
- ENISA provides publications and events which include both perspectives from the private and public sector, improving mutual understanding.

Overall, the case studies confirmed that ENISA has managed to respond to the different needs across Member States and across the academia, and the private and public sector. It also follows from this, that across these stakeholders, some of ENISA´s activities in 2015 were less relevant:

- In some Member States (such as Germany, France, the United Kingdom, Sweden and the Netherlands), ENISA´s work on the cryptographic building blocks is regarded as irrelevant, because it addresses national security issues (for example, in the field of eID), which is regarded as a field of strictly national competence of Member State.
- In some Member States, ENISA´s highly technical reports (for example "Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations"), cannot be used because the national capacity is still too low to implement such solutions.
- For certain stakeholders, some areas of ENISA´s activities were not priority areas for them in 2015, and they were therefore less relevant.

In summary, the case studies show that in terms of relevance, ENISA´s 2015 activities struck a balance between the different needs of stakeholders, which also means that not all activities are relevant to all stakeholders.

4.2 Effectiveness of ENISA's activities: Evaluation findings relating to 2015 Specific Objectives

In the 2015 Work Programme, activities were structured around four strategic objectives, each containing a number of work packages (WPKs) and deliverables. The deliverables correspond largely to what are called core operational activities. This evaluation of effectiveness covers all core operational activities implemented in 2015, with a budget over 30,000 Euro.

The core operational activities in 2015 were structured along four strategic objectives:

- SO1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)
- SO2: To assist the Member States and the Commission in enhancing capacity building throughout the EU
- SO3: To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security
- SO4: To develop and maintain a high level of expertise of EU actors taking into account evolutions in NIS

The information in this section is based on the Work Programme and Annual Activity Report 2015 (draft version), as well as assessments from the stakeholders in the survey and during in-depth interviews. In-depth case studies have been conducted on WPK 1.2, 2.1 and 3.3; the findings of these cases have been integrated into the analysis in relation to these WPKs where relevant.

4.2.1 Overall findings - effectiveness

This section presents the evaluation´s overall findings on effectiveness, across the four SOs for 2015 based on relevant data from the yearly annual survey, interviews with stakeholders, desk research and case studies.

Conclusion on effectiveness

Based on the evidence available, it can be concluded that ENISA´s 2015 activities have been effective across the four SOs, but to different extents. Conclusions are presented for each strategic objective in sections 4.2.2-4.2.5, while this box focuses on the overall effectiveness of the 2015 activities.

Overall, 53% of the indicators (16 out of 30) from the M&E framework were achieved, showing that the activities during 2015 have clearly contributed to achieving some results for each SO, while other results have been achieved to a lesser extent. This picture is also supported by the findings in relation to the degree of achievement of the KIIs (17 out of 28 to date), which show that these targets have been achieved to varying degrees, with some KIIs having more long-terms targets making it too early to judge the degree of achievement and others showing a lack of clarity on the degree of achievement due to what appears to be a lack of follow-up on activities.

In fact, while ENISA´s 2015 activities are contributing to the development and maintenance of a high level of expertise of EU actors, it is doing so to a limited extent. On the one hand, evidence confirms that ENISA´s 2015 activities have provided stakeholders of CIIs 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 evidence collected also points to ENISA´s 2015 activities enhancing capacity building to some extent, and to varying degrees according to the stakeholder type. In this regard, the evaluation finds that ENISA's support has: enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis; allowed for the development of sound and implementable strategies to ensure preparedness, response and recovery; and contributed to developing capacities in prevention, detection, analysis and response in Member States. The evaluation found less evidence confirming that the 2015 activities enhanced the Commission's capacity, and found that ENISA is not well known within the private sector, which goes some way to explaining why it has not contributed to improving the preparedness of the private sector to respond to NIS threats or incidents to a large extent.

In addition, it can be concluded that during 2015 ENISA 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 appears to be more effective at *implementing* than *developing* such policies.

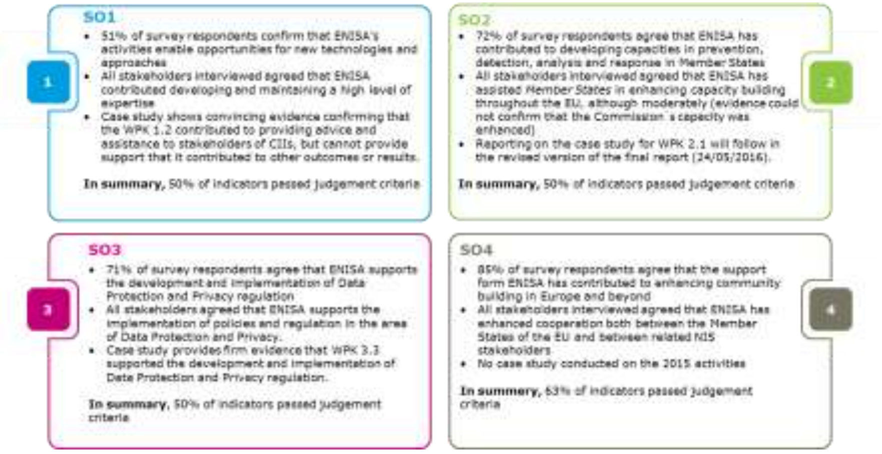
Finally, the evidence gathered suggests that ENISA´s 2015 activities have made an important contribution to enhancing cooperation both between Member States of the EU and between related NIS stakeholders. In extension of this finding it is assessed that ENISA has contributed to a great extent to enhancing community building in Europe and beyond; increased the cooperation of operational communities; and improved services, workflow and communication among stakeholders to respond to crises.

It is worthy of note that while ENISA's organisational set-up, procedures and processes were perceived by stakeholders as being 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;
- The broad mandate and the variety of tasks it seeks to fulfil;
- The lesser involvement of some Member States;
- The informal nature of the NLO network (it is not defined in the ENISA Regulation), meaning that NLOs approach their role differently;
- An apparent lack of a uniform policy when it comes to authorship.

The findings in relation to the four SOs are summarised in the figure below, while the following paragraphs present the evidence in more detail, organised by data source.

Figure 13: Summary of findings by Strategic Objective, 1 to 4



SO1

- 51% of survey respondents confirm that ENISA's activities enable opportunities for new technologies and approaches
- All stakeholders interviewed agreed that ENISA contributed developing and maintaining a high level of expertise
- Case study shows convincing evidence confirming that the WPK 1.2 contributed to providing advice and assistance to stakeholders of CIIs, but cannot provide support that it contributed to other outcomes or results.

In summary, 50% of indicators passed judgement criteria

SO2

- 72% of survey respondents agree that ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States
- All stakeholders interviewed agreed that ENISA has assisted *Member States* in enhancing capacity building throughout the EU, although moderately (evidence could not confirm that the Commission 's capacity was enhanced)
- Reporting on the case study for WPK 2.1 will follow in the revised version of the final report (24/05/2016).

In summary, 50% of indicators passed judgement criteria

SO3

- 71% of survey respondents agree that ENISA supports the development and implementation of Data Protection and Privacy regulation
- All stakeholders agreed that ENISA supports the implementation of policies and regulation in the area of Data Protection and Privacy.
- Case study provides firm evidence that WPK 3.3 supported the development and implementation of Data Protection and Privacy regulation.

In summary, 50% of indicators passed judgement criteria

SO4

- 85% of survey respondents agree that the support form ENISA has contributed to enhancing community building in Europe and beyond
- All stakeholders interviewed agreed that ENISA has enhanced cooperation both between the Member States of the EU and between related NIS stakeholders
- No case study conducted on the 2015 activities

In summery, 63% of indicators passed judgement criteria

As shown in the figure above, the evaluation finds an overall moderate achievement of all four SOs, when all sources of evidence are taken into account. It is important to note that this is a summary, and that the 2015 activities under the SO may have been successful to different extents (the detailed findings for each SO are presented in sections 4.2.2 to 4.2.5).

Detailed findings on effectiveness per data source are presented below.

Interviews

The **assessment of stakeholders across all four stakeholder groups**[32] **was broadly positive concerning the extent to which ENISA achieved its objectives in 2015**. However, it was highlighted by various representatives that certain aspects of the organisation of ENISA impose challenges in the achievement of the objectives set out in its legal mandate. It should be noted that these comments often related to the Agency as a whole, rather than to the 2015 activities specifically. The main challenges mentioned by representatives of the European Commission, the European Parliament, the PSG and the Management Board were:

- The limited resources that ENISA disposes of;
- The broad mandate and the variety of tasks;

[32] Interviews concerning ENISA were conducted with stakeholders belonging to four stakeholder groups: the European Parliament, the European Commission, the Permanent Stakeholder Group (PSG) and the Management Board (MB).

- The lesser involvement of some Member States and;
- The need for the European Commission to reinforce the role of ENISA and make it more operational, granting the Agency more responsibilities in coordinating and supporting the policy objectives in this field.

Generally, **all stakeholders interviewed assessed the organisation of ENISA as being supportive of the achievement of its objectives**. However, certain challenges were highlighted by the various stakeholder groups' representatives. Representatives of the Management Board, the European Commission and the PSG indicated that the limited financial resources available to ENISA and the fact that they are understaffed impose challenges to the achievement of its objectives. In connection to this, two representatives of the Management Board also mentioned that the limited financial resources lead to less attractive expert salaries which make it difficult for ENISA to attract and retain well-qualified experts. These challenges appear to be more general, and although they were present during 2015, they do not relate exclusively to the activities carried out during that year.

Additionally, representatives of the Management Board and the PSG indicated that the geographical location of the Agency imposes difficulties in terms of its efficiency, visibility and awareness/involvement in developments in Brussels. It was also mentioned that closer cooperation with the Member States and the EC was necessary to enhance the visibility of ENISA and ensure full involvement of key stakeholders in its activities. It was mentioned that the most important challenges for ENISA in the following three years will be: supporting the establishment of a CSIRT cooperation network and supporting the NIS Directive and achieving an adequate level of government cooperation. However, in relation to this, the question of limited human resources was reiterated.

While acknowledging the importance of the NLO network, it was also indicated that the position of the NLO network is completely informal and it is not defined in the ENISA Regulation, meaning that NLOs approach their role differently. In fact, while it is recognised that the NLO network is informal and functions on a "best effort basis", there is very limited evidence suggesting that NLOs undertake the tasks envisioned in the terms of reference for the role. Thus, further clarifications could be provided in relation to this. The case study analysis (see below) provides further detail on this.

One representative of the PSG also raised concerns regarding the limited role of the PSG, which currently is limited to an advisory role. The representative of the PSG indicated that ENISA would benefit from further involvement of the PSG in galvanising industry for ENISA or, potentially, from the involvement of PSG in providing expert opinion to the production of deliverables. At the time of writing, the role of the PSG was seen as limited and deliverables are not seen by the PSG before they are published (e.g. SCADA, Good practices for cloud computing in finance sector – where PSG members are heavily involved in the topics but their role in the consultation of ENISA is limited). Thus, the incentive of the PSG to support in their dissemination is relatively low. This challenge may be due to legal constraints in the governance structure of the Agency and the defined role of the PSG.

It was **generally assessed by Management Board representatives that ENISA's procedures and systems are conducive to supporting the achievement of its objectives**.

Representatives of the Management Board also assessed that ENISA has a very pro-active approach and that the Agency provides a forum for cooperation and reaches out to Member States and other stakeholders. This is particularly relevant for Member States that have limited resources, i.e. smaller Member States that do not have the resources to write comprehensive guides. For example, in the case of Ireland, it was noted that the documents produced by ENISA were used to develop the national strategy and the implementation plan associated with the national strategy. Additionally, the use of ENISA input at national level was also noted by a couple of Management Board representatives who used ENISA deliverables to build national strategies.

In terms of deliverables, it is acknowledged that ENISA makes efforts to involve experts from all Member States but there is a challenge as concerns the **authorship of ENISA's deliverables.** It should be noted that for some publications there may be legal constraints that apply to the crediting authors[33]. It appears that there is no common approach or authorship policy which requires ENISA to state the name and the role of the actors involved (authors, supports etc.). In some cases, ENISA takes the full authorship even when others involved, whereas in others a list of authors/experts is included in the deliverable. According to the representative of the Management Board, being mentioned in the deliverables is an important motivating factor for contributing to ENISA. Thus, it was recommended that a policy on the workings of ENISA in this regard should be put in place in order to enhance the transparency of the process.

Case studies

The case studies provided new details on ENISA´s overall effectiveness in 2015, and also gave further details on several findings derived from the survey and in-depth interviews. In addition, this section contains some points which relate to the Agency in more general terms.

Regarding ENISA´s overall effectiveness, the case studies showed that the key achievements were:

- ENISA supported Member States in implementation of regulation, and that the Agency´s 2015 activities have already done so in relation to the implementation of the GDPR (WPK 3.3 case study).
- ENISA´s 2015 activities provided advice and assistance to stakeholder of CII, in particular by collecting and assessing information on security and resilience of major eHealth infrastructures, which raised awareness of risks in using ICT and generating health data (WPK 1.2 case study)
- ENISA disseminated good practices regarding cyber security among public and private organisations through its 2015 publications, workshops and participation in conferences and networks (WPK 2.1 case study).

Based on the case studies, it was hard to identify firm evidence on the extent to which ENISA has delivered the expected results through the WPKs in question. The main reasons for this were that interviewees found it too early to judge and too difficult to identify the exact contribution of ENISA to the results – when efforts where on-going on national level. Additionally, due to the absence of a feedback loop, no evidence is collected on how, for example, ENISA´s publications are used, or how new skills and knowledge for events, exercises or trainings are used.

One of the main inhibitors of ENISA´s effectiveness was identified across all case studies, namely that the dissemination of ENISA´s events and publications should be improved to strengthen the effectiveness of the Agency. Since interviewees highlighted the quality and relevance of ENISA´s publications, several interviewees strongly recommended that ENISA improves their dissemination strategies as soon as possible, and underlines that the Agency´s work is relevant to a much larger audience than currently is aware of it. A strong example of this challenges that out of 12 target group interviewees (excluding interviewees who were ENISA staff and NLOs), all interviewees proactively identified relevant publications themselves, and in some cases had overlooked certain deliverables, which upon hearing about them in the interview stated where relevant to their work. It should be noted that this challenge concerned ENISA's 2015 activities, but that it is unlikely to have been exclusive to that year.

[33] This was brought to the attention of the evaluator by ENISA.

Furthermore, ten target group interviewees where not aware of the presence of an NLO in their country, and in the remaining two cases, the target group interviewee knew the NLO through other channels, but where not aware of his/her function. With regards to the six NLOs interviewed, the awareness of ENISA activities and approach to disseminating information to relevant persons in the Member State (primarily public authorities, bodies and agencies) was unclear. While interviewees suggested that ENISA dissemination activities should encompass several tools (awareness via LinkedIn, presence at conferences and talks etc.), the findings suggest that the usage of the NLO network should be an important tenant in this effort to immediately increase the effectiveness, reach and potential impact of the Agency´s work.

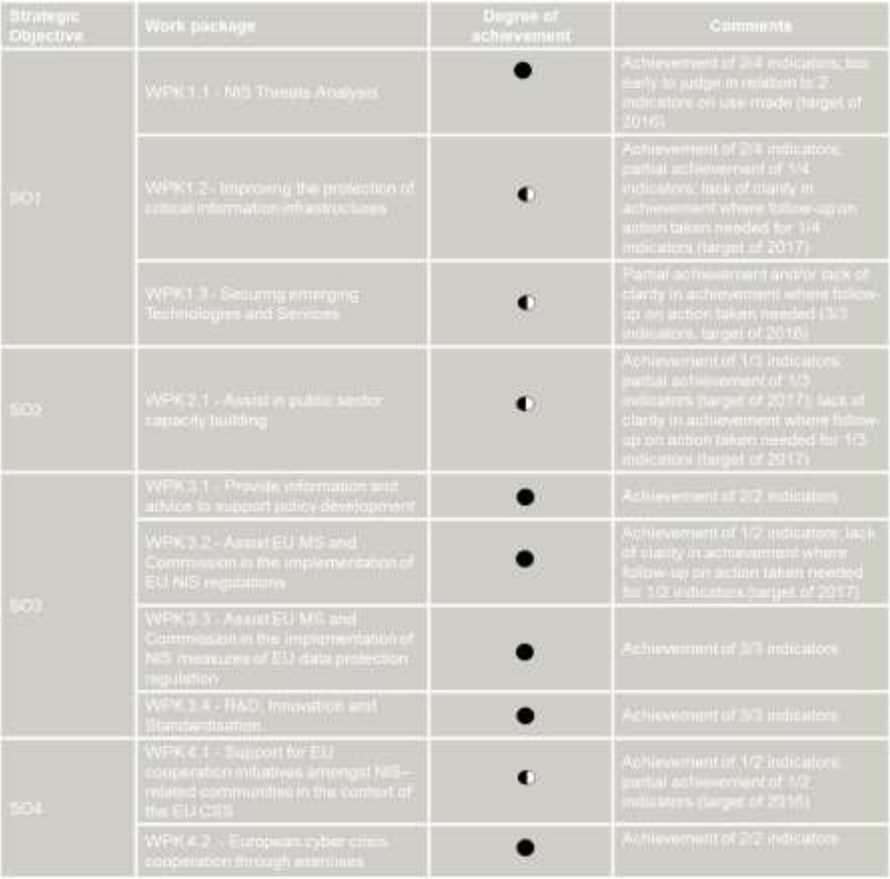
Desk research

The Key Impact Indicators (KIIs) set out in the 2015 Work Programme were achieved to varying degrees by all deliverables, as the table below illustrates. It presents an overview of the degree to which the KIIs have been achieved (to date) on the basis of the detailed assessment per work package and deliverable presented in Appendix 4; the assessment drew on the results presented in the Annual Activity Report 2015 (draft).

Overall, where KIIs were more operational and involved the participation of given experts in an event or drafting of a report, such targets have tended to be achieved. However, as these indicators are not really a measure of the long-term/strategic impact of ENISA’s deliverables, they have not been included in the WPK-specific analysis presented below.

On the other hand, certain of the pre-defined KIIs seek to ascertain whether use has been made of a given ENISA deliverable by stakeholders. In two instances evidence of true impact of a given deliverable was provided, namely in relation to WPK 2.1, D1 and WPK 3.2, D4; this evidence has been included in the analysis below. In a number of cases where the organisation of a workshop or development of a report was intended to lead to action at stakeholder level, e.g. recommendations being used, operational practices being improved or increased familiarisation, it was unclear whether the KIIs were achieved as follow-up with stakeholders on the action taken further to a workshop or development of a report has not been undertaken by ENISA for data presented in the Annual Activity Report 2015 (draft). It is worthy of note that it is unlikely that actual use of reports can be documented and verified at this stage, as many publications became available end 2015 or beginning 2016. As such, it was not possible to integrate any evidence in the analysis below. In other words, for several of the KIIs it is deemed too early to conclude on the extent of their achievements, since it will take time for these effects to manifest themselves.

Table 5: Assessment of the degree of achievement of the KIIs for ENISA deliverables over EUR 30,000



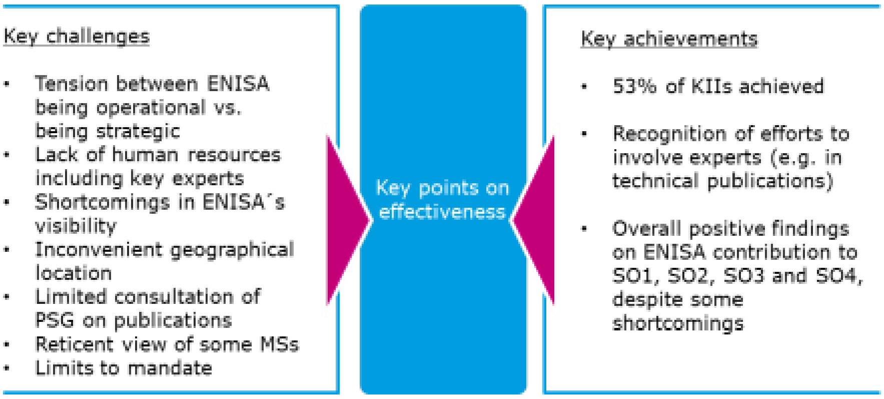
Strategic Objective	Work package	Degree of achievement	Comments
SO1	WPK1.1 - NIS Threats Analysis	●	Achievement of 2/4 indicators; too early to judge in relation to 2 indicators on use made (target of 2016)
	WPK1.2 - Improving the protection of critical information infrastructures	◐	Achievement of 2/4 indicators; partial achievement of 1/4 indicators; lack of clarify in achievement where follow-up on action taken needed for 1/4 indicators (target of 2017)
	WPK1.3 - Securing emerging Technologies and Services	◐	Partial achievement and/or lack of clarity in achievement where follow-up on action taken needed (3/3 indicators, target of 2018)
SO2	WPK2.1 - Assist in public sector capacity building	◐	Achievement of 1/3 indicators; partial achievement of 1/3 indicators (target of 2017); lack of clarity in achievement where follow-up on action taken needed for 1/3 indicators (target of 2017)
SO3	WPK3.1 - Provide information and advice to support policy development	●	Achievement of 2/2 indicators
	WPK3.2 - Assist EU MS and Commission in the implementation of EU NIS regulations	●	Achievement of 1/2 indicators; lack of clarity in achievement where follow-up on action taken needed for 1/2 indicators (target of 2017)
	WPK3.3 - Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation	●	Achievement of 3/3 indicators
	WPK3.4 - R&D, Innovation and Standardisation	●	Achievement of 3/3 indicators
SO4	WPK4.1 - Support for EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS	◐	Achievement of 1/2 indicators; partial achievement of 1/2 indicators (target of 2016)
	WPK4.2 - European cyber crisis cooperation through exercises	●	Achievement of 2/2 indicators

Legend: Degree of achievement[34]:
○ = low ◐ = middle ● = high

The figure below provides an overview of the main challenges and key achievements of ENISA, as derived from the overall findings presented above.

[34] Low = Fewer than 50% of KIIs have been achieved; Middle = The majority of KIIs have been achieved; High = All KIIs have been achieved

Figure 14 Summary of key challenges and key achievements



Key challenges

- Tension between ENISA being operational vs. being strategic
- Lack of human resources including key experts
- Shortcomings in ENISA´s visibility
- Inconvenient geographical location
- Limited consultation of PSG on publications
- Reticent view of some MSs
- Limits to mandate

Key points on effectiveness

Key achievements

- 53% of KIIs achieved
- Recognition of efforts to involve experts (e.g. in technical publications)
- Overall positive findings on ENISA contribution to SO1, SO2, SO3 and SO4, despite some shortcomings

4.2.2 **Strategic objective 1**: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)

Through its first Strategic objective (SO1), ENISA seeks to develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS). It aims to do so by carrying out NIS threats analysis (WPK1.1), Improving the protection of Critical Information Infrastructures (WPK 1.2), Securing emerging Technologies and Services (WPK 1.3) and supporting short- and mid-term sharing of information regarding issues in NIS (WPK 1.4). The overall findings per data collection tool for SO1 and the findings in relation to each of its WPKs are presented below; the box below represents a conclusion in relation to SO1.

Conclusion on SO1

On the basis of the evidence collected, it can be concluded that while ENISA’s 2015 activities under SO1 are contributing to the development and maintenance of a high level of expertise of EU actors, it is doing so to a limited extent. ENISA is considered a “trusted partner” by stakeholders, providing “relevant”, “useful”, “quality” inputs; is contributing to putting in place more effective risk mitigation strategies according to the survey results; and the case study shows convincing evidence confirming that WPK 1.2 contributed to providing advice and assistance to stakeholders of CIIs. However, only 52% of survey respondents agree that technical capacity has increased among involved stakeholders; ENISA was found to promote relevant methods towards emerging technologies and enable opportunities for new technologies and approaches to a limited extent; and it was not possible to demonstrate through the case study that WPK 1.2 contributed to other intended outcomes or results. In fact, this is an objective which is most challenging to fulfil due to Member State (CSIRT) competence and capabilities in this more operational area; ENISA’s more strategic mandate; and the limited resources at ENISA’s disposal. It should also be taken into account that increasing technical capacity among stakeholders will take time to achieve, and that the 2015 activities contribute to this long-term objective.

Detailed findings per data source are presented below.

Survey

A total of 85% of survey respondents are familiar with ENISA’s work on developing and maintaining a high level of NIS expertise (see Appendix 5).

As regards the intended results, the survey findings suggest that:

- ENISA's outputs and deliverables contribute to putting in place more effective risk mitigation strategies, with close to 70% of respondents (68%) either strongly agreeing (23%) or agreeing (45%) with this statement; a detailed breakdown by stakeholder type is presented in Appendix 5.
- ENISA promotes relevant methods towards emerging technologies to a more limited extent, with only 56% of interviewees strongly agreeing (11%) or agreeing (45%) with this statement. There are divergent views per stakeholder group in relation to this statement, with the Management Board, industry and the PSG being comparatively less positive in this regard.
- ENISA's activities also enable opportunities for new technologies and approaches to a more limited extent, with only 52% of interviewees strongly agreeing (13%) or agreeing (38%) with this statement. Similarly to the statement above, the Management Board, industry and the PSG were comparatively less positive in this regard.

The figures in Appendix 5 provide more details on the distribution of respondents.

In-depth interviews

In relation to ENISA's SO1, it was generally reported that **ENISA´s 2015 activities have achieved the goal of developing and maintaining a high level of expertise of EU actors, though various stakeholders indicated that SO1 is the most challenging objective for ENISA to achieve**. As a result, the interviews revealed some shortcomings which relate to the Agency in general, rather than to the 2015 activities specifically. Stakeholders' assessment of the extent to which ENISA´s 2015 activities helped in the development and maintenance of the level of expertise of EU actors in relation to the evolutions in NIS offered a mixed picture.

One EP representative indicated that ENISA's role in developing a high level of expertise of EU actors has increased and ENISA is highly active in this field. According to the EP representative, ENISA is increasingly perceived both by the EC and the industry as a "trusted partner". However, in this regard, the respondent also indicated that more could be done in making ENISA's mandate more operational, in the sense of granting ENISA more responsibilities for coordinating Member States in cyber security. The EP representative also highlighted certain limitations in connection to the current ENISA mandate and the resources ENISA disposes of.

Similarly, the European Commission representatives emphasised that the Agency does not dispose of sufficient human resources and the salaries are not attractive enough to attract new talent. Additionally, according to the European Commission representatives, ENISA generally managed well in providing expertise, but due to lack of resources and the variety of areas that the Agency covers, the Agency tends to focus on many small projects to meet expectations of all stakeholders. In this sense, it was recommended that the approach should be re-thought and the focus should be narrower, e.g. focus on treat landscape analysis, and cyber exercises. In addition, the European Commission representatives also indicated that ENISA should continue to closely cooperate with CERTs. In the view of one European Commission representative, this constitutes a challenge for ENISA and better synergies between ENISA and CERT EU could be built in order to foster a higher level of expertise of EU actors on NIS. In relation to closer cooperation with the CERTs, one representative of the Management Board stressed, ENISA' role should remain on a strategic level supporting and facilitating cooperation, whereas CERT EU should be operating at the operational level.

The PSG representatives assessed that ENISA's involvement in the field leads to capacity building across Europe, as particular bodies and trade associations are provided with advice and guidance (e.g. aviation, transport systems, e-Health 2015, smart grids, and EID). At the same time, representatives of the PSG had mixed views in relation to the extent to which ENISA contributed to building a high level of expertise of EU actors. On the one hand, one of the representatives of the PSG indicated the ENISA disposes of a high level of expertise which is comparable to the technical agencies of this sort that Member States have at national level. On the other hand, the other PSG representative assessed that on an operational level, ENISA does not dispose of a comparatively high level of expertise as the CERTs are much more qualified in providing training. A concrete example was provided to substantiate the assessment of a relatively low contribution of ENISA to a high level of expertise of EU actors in NIS, i.e. the fact that in the case of the NIS Directive, Member States and national level institutions addressed questions to industry stakeholders for clarification, which, according to his assessment should have been clarified by ENISA.

The assessment of the Management Board representatives was generally positive and interviewed stakeholders indicated that ENISA has added value by contributing to capacity building through specific technical studies. The material on CERT capacity building and cyber security provided by ENISA was assessed as highly valuable and of high quality. Representatives of the Management Board also indicated that ENISA has a pivotal role in supporting Member State to attain a better understanding of the needs, challenges and constraints of actors and helping them build better policies. For example, according to one representative, ENISA had a pivotal role in supporting the Telecom Package work and had a valuable input to Cyber Europe (work on SOPs).

However, certain general challenges were noted by representatives of the Management Board in relation to ENISA's mandate which limits its role in building expertise to a passive one (providing expertise through studies, annual reports, threat landscape papers etc.), although ENISA also supports training activities. Hence, a more active/operational role of ENISA in this area was called for by two stakeholders and it was stated that it should be accompanied by an increase in resources. As a general comment, other representatives of the Management Board raised concerns about the added value that ENISA brings concerning operational response to incidents and technical expertise on threats, considering the high level of expertise existent at national level in connection to cyber security and crypto security (i.e. academia and government capacity at national level).

The representatives of the Management Board also had mixed opinions concerning the achievement of SO1. The contribution of ENISA to the development and maintenance of a high level of expertise of EU actors was fully acknowledged by the interviewed representatives of the Management Board and various interviewees highlighted:

- The usefulness of the deliverables of ENISA both in operational terms and in developing national; documents (e.g. cryptography studies);
- The high quality independent analysis and technical policy level;
- The unique capacity of ENISA to bring together various actors and bodies across the world.

In addition to this, one representative of the Management Board emphasised the reliability of ENISA in providing support to Member States, when prompted to do so. For example, one representative of the Management Board provided the example of a request issued to ENISA under Article 14, whereby ENISA was asked to help determine the type of models for governance of cyber security for Poland. The response of ENISA was assessed as being both prompt and a high quality output.

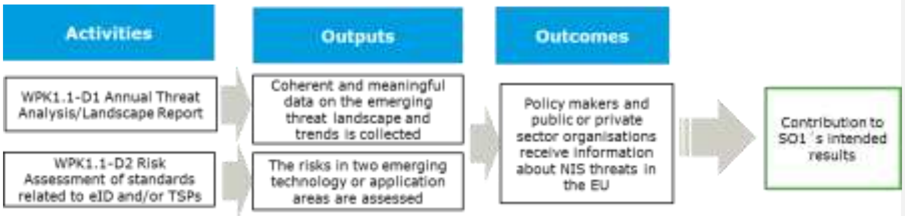
Case study

In relation to SO1, a case study on WPK 1.2 was conducted as part of the evaluation. The findings from it are described in section 4.2.2.2 below.

4.2.2.1 Work Package 1.1: NIS Threats Analysis

WPK 1.1 aimed to collect and collate current data in order to develop the ENISA threat landscape, including current threats and threat trends in NIS and emerging technologies. This evaluation focussed on two deliverables within this WPK, namely the "Annual Threat Analysis / Landscape Report (Q4, 2015)" (D1) and the "Risk Assessment on two emerging technology / application areas" (D2). The figure below provides an overview of which outputs and outcomes each deliverable under WPK 1.1 was intended to deliver in order to contribute to the achieving the intended results under SO1.

Figure 15: Simplified intervention logic for WPK 1.1


Activities
Outputs
Outcomes
WPK1.1-D1 Annual Threat Analysis/Landscape Report
WPK1.1-D2 Risk Assessment of standards related to eID and/or TSPs
Coherent and meaningful data on the emerging threat landscape and trends is collected
The risks in two emerging technology or application areas are assessed
Policy makers and public or private sector organisations receive information about NIS threats in the EU
Contribution to SO1´s intended results

The key findings from the interviews suggest that the deliverables under WPK 1.1 were assessed as useful, and D1 was highlighted by several stakeholders (EC, PSG and Management Board) as one of ENISA core deliverables, which succeeded at delivering its intended output (collecting data on emerging threat landscape). Overall, policy makers and private sector organisation were assessed to have received information about NIS threats in the EU (the WPK´s intended outcome). In part the fact that the publication is made available on an annual basis, encourages usage amongst stakeholders, who begin to rely on it as a credible and stable source of information.

A high proportion of survey respondents (80% in total) confirm that the work undertaken by ENISA on NIS threats in the EU are relevant and of high quality, and 75% of survey respondents agree that ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions, as further illustrated in the figures below (see Appendix 5).

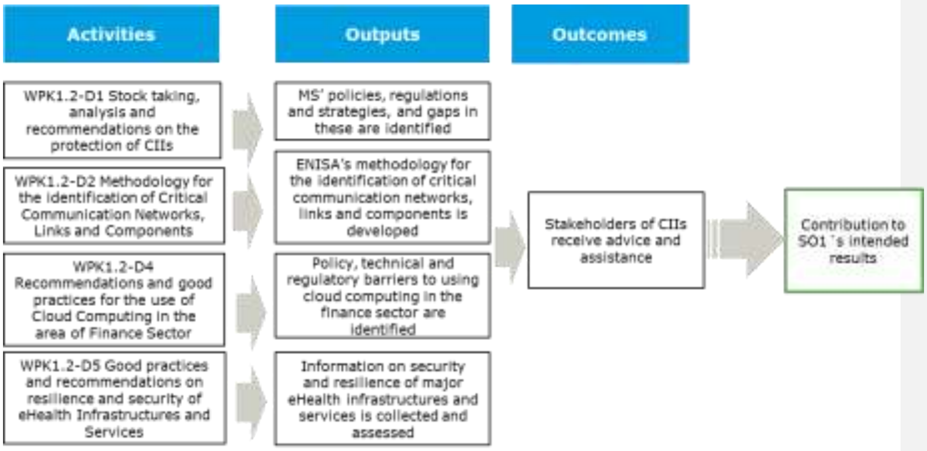
4.2.2.2 Work Package 1.2: Improving the protection of CIIs

Through WPK 1.2, ENISA aimed at providing advice and assistance on request to targeted stakeholders of Critical Information Infrastructures (CIIs) by:

- Taking stock of Member State policies, regulations and strategies including international frameworks (e.g. US NIST) and identify gaps related to CIIs.
- Cooperate with public and private stakeholders to identify good practices, collect and analyse requirements and issue recommendations for improving the way Member State address the protection of CIIs.

The figure below provides an overview of which outputs and outcomes each of the four deliverables under WPK 1.2 was intended to deliver in order to contribute to the achieving the intended results under SO1.

Figure 16: Simplified intervention logic for WPK 1.2


Activities
Outputs
Outcomes
WPK1.2-D1 Stock taking, analysis and recommendations on the protection of CIIs
WPK1.2-D2 Methodology for the identification of Critical Communication Networks, Links and Components
WPK1.2-D4 Recommendations and good practices for the use of Cloud Computing in the area of Finance Sector
WPK1.2-D5 Good practices and recommendations on resilience and security of eHealth Infrastructures and Services
MS' policies, regulations and strategies, and gaps in these are identified
ENISA's methodology for the identification of critical communication networks, links and components is developed
Policy, technical and regulatory barriers to using cloud computing in the finance sector are identified
Information on security and resilience of major eHealth infrastructures and services is collected and assessed
Stakeholders of CIIs receive advice and assistance
Contribution to SO1´s intended results

In comparison with the survey, interviewees were a bit more cautious in their assessment of ENISA´s direct contribution to improving the protection of Critical Information Infrastructure. Across different stakeholder categories, interviewees assessed ENISA´s contribution to CII more conservatively, and stated that that considering the high level of expertise existent at national level in connection to cyber security and crypto security (i.e. academia and government capacity at national level)[35], ENISA´s contribution is limited. At the same time, interviewees noted that due to ENISA´s mandate and available resources, the Agency is well placed to provide high-quality technical analysis, and bring together stakeholders, thereby supporting capacity building and ultimately making a contribution to improving the protection of CII.

More or less one third of those surveyed had made use of the deliverables with a value of over EUR 30,000 which fall within this WPK, while between 44% and 50% had not made use of these deliverables; the table below provides an overview of the situation (a more detailed breakdown is presented in Appendix 5).

Table 6: Use made of given deliverables under WPK 1.2

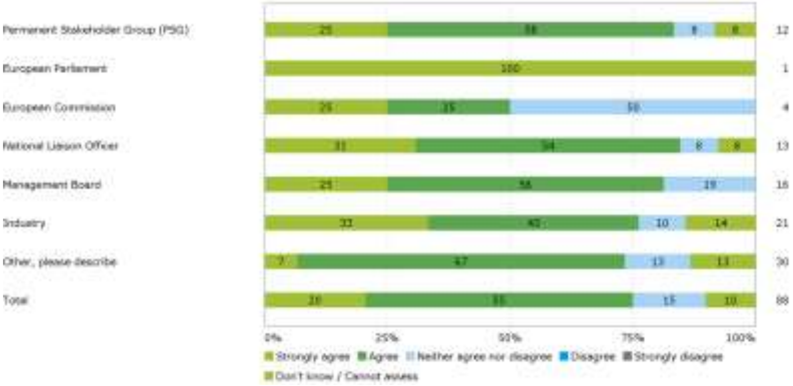
Deliverable	Degree to which use was made of given deliverables (% that answered "Yes")
Stocktaking, Analysis and Recommendations on the Protection of CIIs	32%
CIIP Governance in the European Union Member States" (Annex to "Stocktaking, Analysis and Recommendations on the Protection of CIIs ")	33%
Methodology for the Identification of Critical Communication Networks, Links, and Components" (also known as "Communication network independencies in smart grids ")	34%
Secure Use of Cloud Computing in the Finance Sector. Good Practices and Recommendation	37%
Security and Resilience in eHealth. Security Challenges and Risks	28%

Moreover, in relation to this work package, three quarters (75%) of survey respondents agree that ENISA's work, outputs and publications provide stakeholders of CIIs with relevant advice and assistance, as the figure below further illustrates.

[36] Interviewees were either not willing/able to provide an assessment or were pressed for time.

Deleted: ¶

Figure 17: Q7.15 ENISAS's work, outputs and publications provide stakeholders of CII with advice and assistance



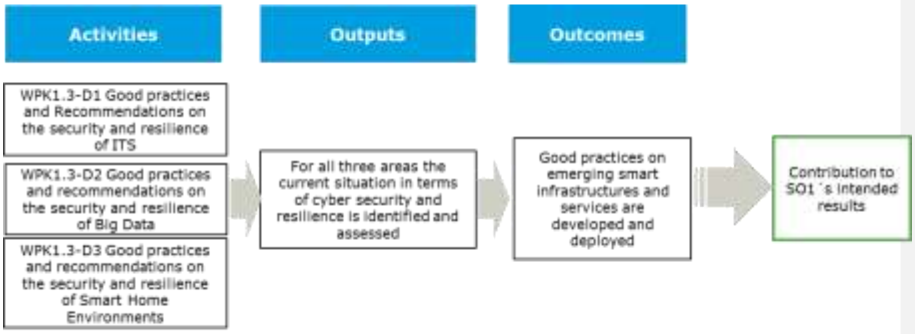
The case study findings also reflect that WPK 1.2 provided advice and assistance to stakeholder of CII, in particular by collecting and assessing information on security and resilience of major eHealth infrastructures, which raised awareness of risks in using ICT and generating health data. The findings indicated that in some cases this outcome is not reached, because some deliverables (e.g. Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services), the reports often tended to be too technical to be relevant at policy level. One of them suggested that ENISA should develop more simple documents on good practices that could more easily be handed over to hospitals themselves, instead of only addressing the technical specialists. Often it would be difficult to understand and then implement ENISA's recommendations. Another of these respondents suggested adding non-technical executive summaries to the reports that could also be used by policy makers.

Further details on the case study findings and methodology can be found in the separate annex attached to this report.

4.2.2.3 Work Package 1.3: Securing emerging Technologies and Services

This WPK aims to develop good practices on emerging smart infrastructures and services and work with relevant stakeholders to deploy them at an early stage of adoption. The areas concerned are intelligent transportation systems, Smart Home environments as well as Big Data and corresponding services used for offering critical services. The figure below provides an overview of which outputs and outcomes each deliverable under WPK 1.3 was intended to deliver in order to contribute to the achieving the intended results under SO1.

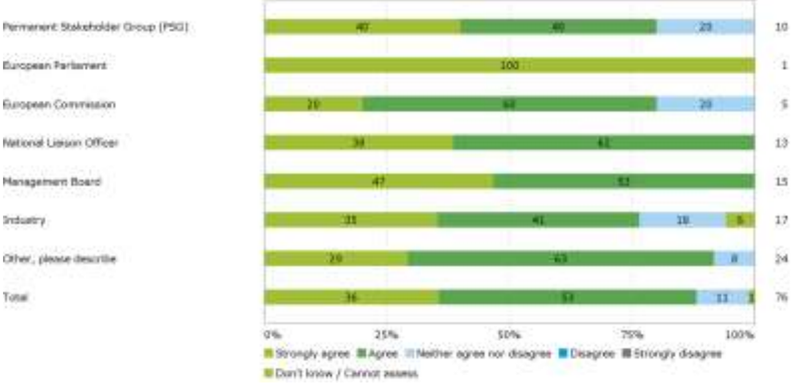
Figure 18 Simplified intervention logic for WPK 1.3


Activities
Outputs
Outcomes
WPK1.3-D1 Good practices and Recommendations on the security and resilience of ITS
WPK1.3-D2 Good practices and recommendations on the security and resilience of Big Data
WPK1.3-D3 Good practices and recommendations on the security and resilience of Smart Home Environments
For all three areas the current situation in terms of cyber security and resilience is identified and assessed
Good practices on emerging smart infrastructures and services are developed and deployed
Contribution to SO1´s intended results

Interviewees suggested that ENISA has definitely produced and disseminated relevant publications, and pointed to this having improved stakeholders ability in assessing their challenges and opportunities in relation to cyber security and resilience (intended output). However, the evidence could not support or reject that this has led to food practices on emerging smart infrastructures and services being developed and deployed (intended outcome), making it difficult to conclude on the WPK´s contribution.

The survey findings suggest that a total of 88% of those surveyed either strongly agree or agree that good practices in NIS have been disseminated by ENISA, which is a strong endorsement of one of the key intended outputs of this WPK.

Figure 19: Q 1.4 Good practices in NIS have been disseminated by ENISA



4.2.2.4 Work Package 1.4: Short- and mid-term sharing of information regarding

No core operational activities of a value of over EUR 30,000 fell within this WPK, so it was not included in the scope of this year’s study.

4.2.3 **Strategic objective 2**: To assist the Member States and the Commission in enhancing capacity building throughout the EU

Through its second Strategic objective (SO2), ENISA seeks to assist the Member States and the Commission in enhancing capacity building throughout the EU. It aims to do so by assisting in public sector capacity building (WPK2.1); assisting in private sector capacity building (WPK 2.2);

and assisting in improving awareness of the general public (WPK 2.3). The overall findings per data collection tool for SO2 and the findings in relation to WPK 2.1 are presented below (the other two WPKs did not have any deliverables above EUR 30,000 so fall outside the scope of this evaluation); the box below represents a conclusion in relation to SO2.

Conclusion on SO2

The evidence collected points to the fact that ENISA's 2015 activities under SO2 have managed to enhance capacity building to some extent, and to varying degrees according to the stakeholder type. The survey results indicate that ENISA's support has: enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis; allowed for the development of sound and implementable strategies to ensure preparedness, response and recovery; and contributed to developing capacities in prevention, detection, analysis and response in Member States. The findings further suggest that ENISA has assisted in enhancing the capacity of Member States (most notably smaller Member States) in particular through: the pivotal role it plays in bringing different actors together and building networks; the dissemination of good practices; the organisation of training sessions (e.g. CSIRT) on a technical level; and its work on NCSS which has acted as an inspiration for certain Member State strategies, etc. 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. The evidence could not confirm that the EU institutions' capabilities in terms of prevention, detection, analysis and response had been enhanced, and the survey findings suggest that ENISA is not well known within the private sector, which goes some way to explaining why it has not contributed to improving the preparedness of the private sector to respond to NIS threats or incidents to a large extent.

At the same time, the findings presented in section 4.1, show that ENISA is addressing a need, since more work needs to be done, as cyber security challenges are not being as adequately addressed as they could be by Member States and in the EU; It should be noted that while this report focusses on the evaluation of the 2015 activities, this conclusion shows that cyber security challenges are under constant development and must therefore be addressed continuously.

Detailed findings per data source are presented below.

Survey

A total of 79% of survey respondents were familiar with ENISA's work to support the capacity building of EU Member States and public and private sectors, as well as its efforts to contribute to raising the level of awareness of EU citizens (see Appendix 5).

As regards the second SO's intended results, the survey findings suggest that:

- ENISA's support has enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis, with 68% of respondents either strongly agreeing (26%) or agreeing (42%) with this statement.
- Sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA; 70% of those surveyed either strongly agreed (21%) or agreed (49%) with this statement.
- More work needs to be done, as cyber security challenges are not being as adequately addressed as they could be by Member States and in the EU, with only 41% of respondents suggesting that this was the case in Member States and 45% in the EU. That said, it is worthy of note that in last year's survey the figure in relation to the EU was much lower at 29%.
- ENISA's activities ensure adherence to EU Data Protection Legislation to a more limited extent, with 59% of respondents either strongly agreeing (17%) or agreeing (42%) with this statement.

A detailed breakdown of each of these findings by stakeholder type is presented in Appendix 5.

In-depth interviews

In connection to ENISA's SO2, most representatives of the Management Board were pleased with the level of training and capacity building that ENISA offered during 2015, but some indicated that there could be room for expanding the trainings the Agency offers and sponsors. Additionally, the pivotal role of ENISA in bringing different actors together was emphasised by several representatives of the Management Board. The representatives of the Management Board indicated that ENISA acts as a forum for cooperation which is particularly important for smaller Member States, as it allows them to learn from the best practice of other states and build their capacity.

Members of the Management Board provided an assessment of the role of ENISA in capacity building and highlighted that ENISA has contributed to this through training sessions on a technical level and through building networks and proactively developing relationships with Member States. The support of ENISA was assessed as highly valuable, in particular by smaller Member States (i.e. Estonia, Ireland) where the institutions find it is difficult to provide training for people in the field. In cases such as these, ENISA role in providing training necessary and creating networking opportunities for the exchange of know-how was assessed as highly valuable. Other Member States have also highlighted the substantial involvement of ENISA in CSIRT community and Cyber Europe as a way to assist in capacity building. It was indicated that Cyber Europe is one of the flagship products of ENISA and it is generally considered a good example of building capacity in practice.

According to one EP representative, the ITRE Committee would want a stronger role for ENISA in connection to this SO, for example in boosting the role of ENISA in building cooperation with external stakeholders in the field of standardisation (e.g. US/EU). This interviewee also indicated that ENISA has strengthened its cooperation with the industry and between industry and public authorities, in larger countries. In smaller countries, ENISA has a more direct capacity building role/effect.

Both representatives of the PSG highlighted that one of the main contributions of ENISA to capacity building throughout the EU was provided through CERT training and the compilation of best practices concerning CERTs during 2015. However, apart from this, the PSG representatives assessed that the contribution to capacity building of ENISA was limited, although its activities have supported awareness raising and dissemination of information across stakeholder groups. This was exemplified by the Good Practices on security and resilience of big data services which it was said had limited visibility amongst stakeholders. In relation to this, it was highlighted that further engagement of the industry would lead to more promotion and dissemination of ENISA's activities to the target community. Other Member States also highlighted the substantial involvement of ENISA in the CSIRT community and Cyber Europe as a way to assist in capacity building. It was indicated that Cyber Europe is one of the flagship products of ENISA and it is generally considered a good example of building capacity in practice.

The European Parliament and the European Commission representatives did not provide an assessment to this question, and their main assessment is presented in section 4.2.1 above. [36]

Case study

In relation to SO2, a case study on WPK 2.1 was conducted as part of the evaluation. The findings from it are described in section 4.2.3.2 below.

4.2.3.1 Work Package 2.1: Assist in public sector capacity building

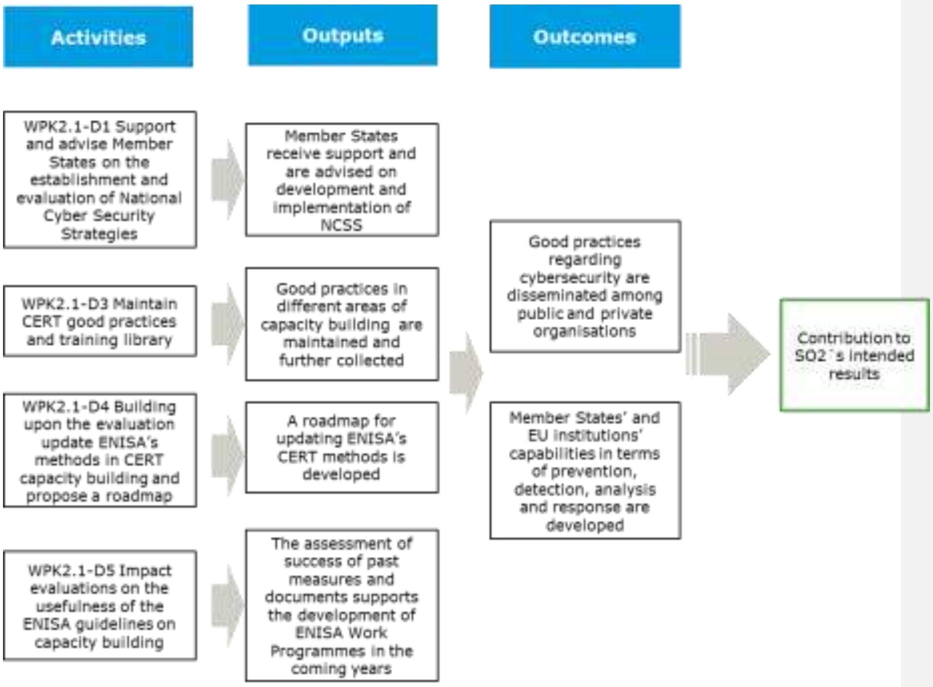
WPK 2.1 aims to help EU Member States and other stakeholders, such as EU Institutions and bodies, to develop and extend the necessary capabilities to meet the ever growing challenges to

[36] Interviewees were either not willing/able to provide an assessment or were pressed for time.

NIS. The stakeholders can be both public such as the Commission or Member States, and private, like banks, SMEs or eHealth providers.

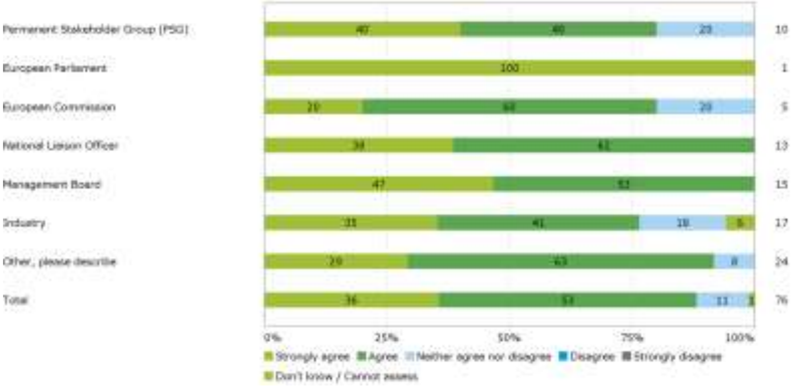
A special emphasis in this WPK is laid on supporting operational bodies and communities (namely CERTs, but other communities where appropriate) by concrete advice (like good practice material) and concrete actions (like CERT training). The figure below provides an overview of which outputs and outcomes each deliverable under WPK 1.2 was intended to deliver in order to contribute to the achieving the intended results under SO2.

Figure 20 Simplified intervention logic for WPK 2.1


Activities
Outputs
Outcomes
WPK2.1-D1 Support and advise Member States on the establishment and evaluation of National Cyber Security Strategies
Member States receive support and are advised on development and implementation of NCSS
WPK2.1-D3 Maintain CERT good practices and training library
Good practices in different areas of capacity building are maintained and further collected
WPK2.1-D4 Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap
A roadmap for updating ENISA's CERT methods is developed
WPK2.1-D5 Impact evaluations on the usefulness of the ENISA guidelines on capacity building
The assessment of success of past measures and documents supports the development of ENISA Work Programmes in the coming years
Good practices regarding cybersecurity are disseminated among public and private organisations
Member States' and EU institutions' capabilities in terms of prevention, detection, analysis and response are developed
Contribution to SO2´s intended results

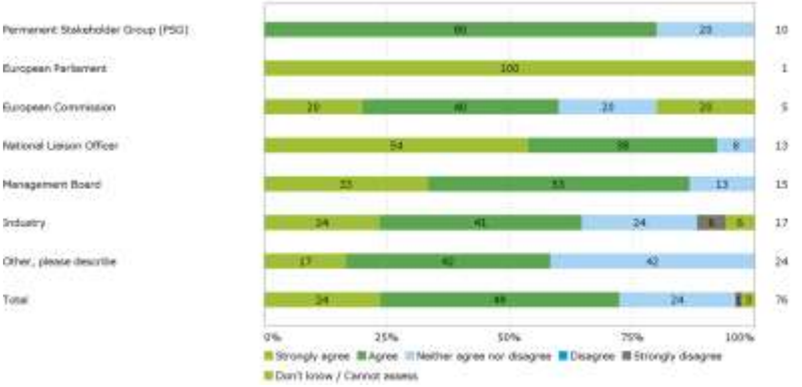
The survey findings suggest that a total of 88% of those surveyed either strongly agree or agree that good practices in NIS have been disseminated by ENISA, which is a strong endorsement of one of the key intended outputs of this WPK.

Figure 21: Q 1.4 Good practices in NIS have been disseminated by ENISA



Moreover, 72% of survey respondents agreed that ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States, with the European Commission and industry being slightly less positive in their judgement than other stakeholder types. While this figure remains above the 70% threshold sought, so can be judged a positive finding, it is worthy of note that in last year's survey, a higher proportion (81%) either strongly agreed or agreed with this statement.

Figure 22: Q 3.3 ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States



A varying proportion of those surveyed had made use of the deliverables with a value of over EUR 30,000 which fall within this WPK, as the table below illustrates (a more detailed breakdown is presented in Appendix 5).

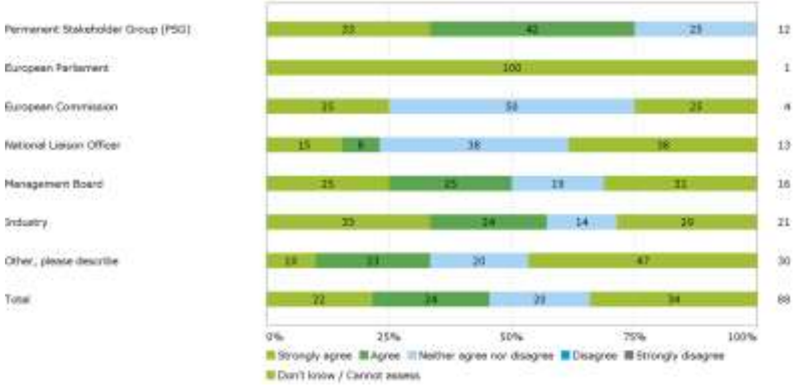
Table 7: Use made of given deliverables under WPK 2.1

Deliverable	Degree to which use was made of given deliverables (% that answered "Yes")
Mobile Threats Incident Handling. Handbook, Document for Teachers	32%
Advanced Dynamic Analysis. Handbook, Document for Teachers	16%
Advanced Static Analysis. Handbook, Document for Teachers	15%

Good practice Guide on Vulnerability Disclosure. From Challenges to Recommendations	47%
Leading the Way. ENISA's CSIRT-related Capacity Building Activities. Impact Analysis - Update 2015	48%

Furthermore, those surveyed were asked whether ENISA's workshop on "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA event" helped disseminate good practices regarding cyber security among private and public stakeholders; 45% of those who responded to the question stated that it has done so by either strongly agreeing or agreeing with the statement.

Figure 23: Q 7.18 ENISA's workshop on "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA event" has helped disseminate good practices regarding cyber security among private and public stakeholders



Finally, it is important to note in relation to the deliverable D1 "Support and Advise Member States on the establishment and evaluation of National Cyber Security Strategies (NCSS)" that the KII whereby "eight Member States use ENISA's recommendations and good practices on NCSS by 2017" had been partially achieved. In fact, as at November 2015 and as further presented in Appendix 4, four Member States had created their national cyber security strategy based on ENISA recommendations, pointing to a direct impact of ENISA's activities. This finding is corroborated by the case study which shows that D1 has given public and private stakeholders opportunities to network and discuss perspectives on the implementation of NCSS, which demands efforts from both sides. However, there is no direct evidence to suggest that any of the deliverables have made a contribution to enabling them to coordinate or cooperate with each other during a cyber-crisis.

In addition, the case study finds that WPK 2.1´s contribution to developing sound and implementable strategies to ensure preparedness, response and recovery, the case study indicates that D1, D3 and D4 have made contributions to disseminating good practices regarding cyber securities. In particular, D1 is suggested to have made a strong contribution to the development and implementation of NCSS which are intended to improve preparedness, response and recovery.

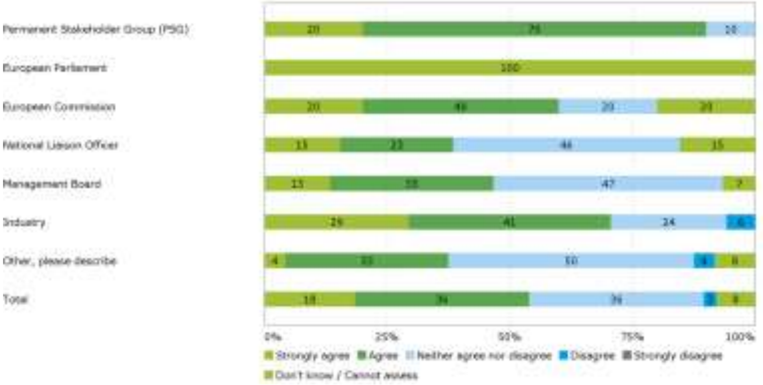
Please note that there were no interview findings which related specifically to this WPK – more general findings can be found in section 4.2.3 on public sector capacity building.

4.2.3.2 Work Package 2.2: Assist in private sector capacity building

No core operational activities of a value of over EUR 30,000 fell within this WPK, so it was not included in the scope of this year's study. That said, to ensure continuity with last year's survey, a question was asked on the extent to which ENISA has contributed to improving the preparedness of the private sector, the results of which are presented below.

Only 54% of survey respondents agree that ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or accidents.

Figure 24: Q 3.4 ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or incidents



In fact, industry respondents indicate that the work of ENISA is not well known in the private sector:

> *"I think the output from ENISA is excellent. However, some Member States ignore it, while ENISA is not known in the corporate space therefore the advice is lost"*
>
> *"When I mention ENISA in various meetings/conferences I often get blank stares as to who ENISA are"*[37]

4.2.3.3 Work Package 2.3: Assist in improving awareness of the general public

No core operational activities of a value of over EUR 30,000 fell within this WPK, so it was not included in the scope of this year's study.

4.2.4 **Strategic objective 3**: To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security

By implementing the activities under SO3, ENISA aims to assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security. In its work programme, ENISA commits to helping Member States and the Commission with implementing privacy and data protection measures through privacy strategies and new business models. It aims to do so by providing information and advice to support policy development (WPK 3.1); assisting EU Member State and the Commission in the implementation of EU NIS regulations (WPK 3.2); assist EU Member State and the Commission in the implementation of NIS measures of EU data protection regulation (WPK 3.3); and supporting R&D, Innovation and Standardisation (WPK 3.2). The

[37] Quotes taken from Question 3.11

overall findings per data collection tool for SO3 and the findings in relation to each of its WPKs are presented below; the box below represents a conclusion in relation to SO3.

Conclusion on SO3

On the basis of the evidence collected in relation to SO3, it can be concluded that in 2015 ENISA 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 appears to be more effective at *implementing* than *developing* such policies. The support ENISA provides to the development and implementation of Data Protection and Privacy regulation and its work, outputs and publications were found to positively contribute to ensuring personal data protection and secure services, and to setting standards for NIS and privacy. In particular, the input provided by ENISA to implement new policies for NIS in the EU was found useful. Concrete examples provided did not relate to 2015 in particular but included its work on the Telecoms package, the NIS Directive and in relation to Article 13a. However, the interviews allowed for such findings to be nuanced, suggesting that ENISA plays an important role in the *implementation* of policies related to NIS by capitalising on its thorough understanding of the legal basis, the technical context, and stakeholders' views, but that it could play a larger role in the *development* of policies through increased coordination with the European Commission and Member States. Limited resources were again seen as a limiting factor to the role ENISA can play in relation to this objective, as well as the European Commission's perception of ENISA's role in relation to the implementation and development of such policies.

Detailed findings per data source are presented below.

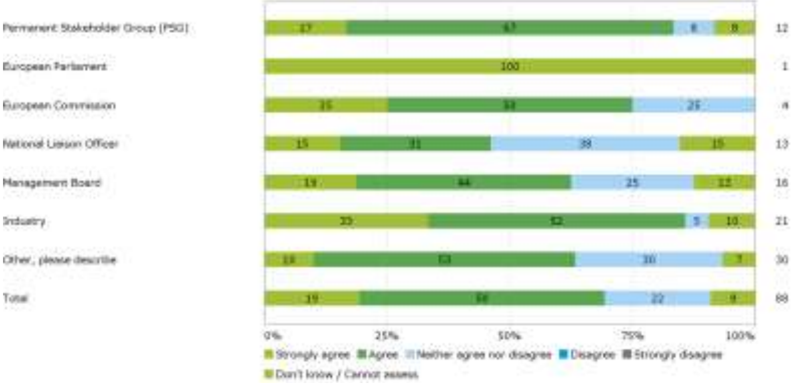
Survey

In relation to the third SO's intended results, the survey findings suggest that:

- ENISA's outputs and deliverables positively contribute to ensuring personal data protection and secure services, with 68% of respondents being of this opinion (very close to the 70% threshold).
- ENISA's outputs and deliverables also positively contribute to setting standards for NIS and privacy; 69% of those surveyed were of this opinion (again very close to the 70% threshold), with 23% strongly agreeing with the statement and a further 46% agreeing; see Appendix 5 for a breakdown by stakeholder.
- ENISA increases coherence between EU funded R&D projects and the objectives of NIS policy to a limited extent, with only 47% of survey respondents (strongly) agreeing with this statement. Stakeholders' views were mixed in this respect, with the PSG and European Commission respondents being more of the opinion that it does so.

Finally, the survey asked respondents whether ENISA's work, outputs and publications have supported the development and implementation of EU regulation in the area of data protection and privacy; 70% of respondents (strongly) agreed that this was the case with the PSG, industry and European Commission being more of this opinion than other stakeholder types, as the figure below illustrates.

Figure 25: Q 7.17 ENISA's work, outputs and publications have supported the development and implementation of EU regulation in the area of data protection and privacy



In-depth interviews

The opinions of stakeholders on the role and contribution of ENISA in attaining SO3's goal to assist the Member States and the Commission in developing and implementing the policies were diverse.

It was generally agreed that ENISA has an important role in the implementation of policy initiatives, as evidenced by previous achievements – e.g. Telecom framework – where ENISA was praised for the guidance provided around the framework. In the opinion of representatives of PSG and Management Board, ENISA's thorough understanding of the legal basis, as well as the technical context, the regulators', academia and government views, make it well positioned to provide advice on the implementation of the NIS legal requirements. ENISA provides two things: expert advice on how to implement legislation and a forum to the development of policies. This view was shared by both PSG and Management Board representatives.

However, on the development of the policies, the involvement of ENISA was assessed as minor by most representatives interviewed, and more coordination of European Commission and Member States with ENISA was urged. For example, it was considered crucial for ENISA to participate in working groups, such as the one constituted by DG ENER on cyber security in the energy sector, as this would allow ENISA to ensure a consistent approach in various sectors with approach put forward in NIS directive.

One representative of the PSG indicated that ENISA has assisted the Commission with work on the Telecom framework, NIS Directive and that it is envisaged that it will support with the implementation of the GDPR and EIDAS. However, the representative also indicated that the more ENISA will be involved, the more its resources will be strained. This was reinforced by representatives of the Management Board, who indicated that ENISA does support the Commission and Member States in this regard, keeping within the limits of its mandate. For example, one Management Board representative indicated that ENISA's role is truly built into the NIS Directive.

The European Commission representatives also acknowledged the support of ENISA in the development and implementation of policies but they highlight the lack of resources that affects the involvement of ENISA and at the same time expressed a preference for ENISA to do more to support the Commission in terms of the certification, and assessment schemes for cyber security.

However, one EP representative indicated that the role of ENISA in this regard is regrettably limited due to the fact that the European Commission views ENISA as a supporting actor and not as playing a central role.

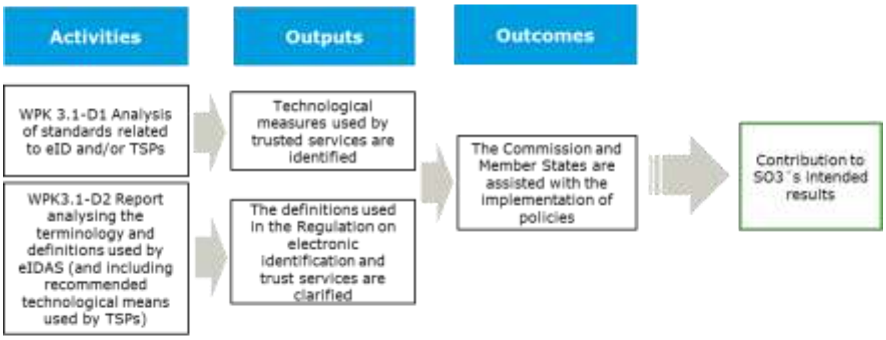
Overall, the interviews suggest that ENISA role is the most important when it comes to supporting implementation rather than actual development of policies.

Case study
In relation to SO1, a case study on WPK 3.3 was conducted as part of the evaluation. The findings from it are described in section 4.2.4.3 below.

4.2.4.1 Work Package 3.1: Provide information and advice to support policy development

This WPK aims at supporting work on regulation especially in the area of eID. The figure below provides an overview of which outputs and outcomes each deliverable under WPK 3.1 was intended to deliver in order to contribute to achieving the intended results under SO1.

Figure 26: Simplified intervention logic for WPK 3.1


Activities
Outputs
Outcomes
WPK 3.1-D1 Analysis of standards related to eID and/or TSPs
WPK3.1-D2 Report analysing the terminology and definitions used by eIDAS (and including recommended technological means used by TSPs)
Technological measures used by trusted services are identified
The definitions used in the Regulation on electronic identification and trust services are clarified
The Commission and Member States are assisted with the implementation of policies
Contribution to SO3´s intended results

A total of 75% of survey respondents agree that the input provided by ENISA to develop new policies for NIS in the EU is useful, and 73% of survey respondents agree that the input provided by ENISA to implement new policies for NIS in the EU is useful. In both instances, industry was slightly less positive in its judgement than other stakeholders, as the figures below illustrate. In relation to the latter point, it is worthy of note that only 61% of respondents (strongly) agreed that the input provided by ENISA to implement new policies for NIS in the EU was useful in last year's survey, thereby strengthening this positive result considering a broader stakeholder base was consulted this year.

Figure 27: Q 2.4 The input provided by ENISA to develop new policies for NIS in the EU is useful

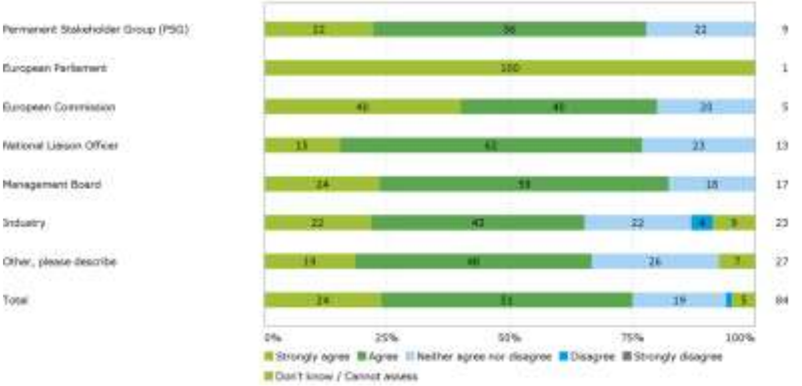
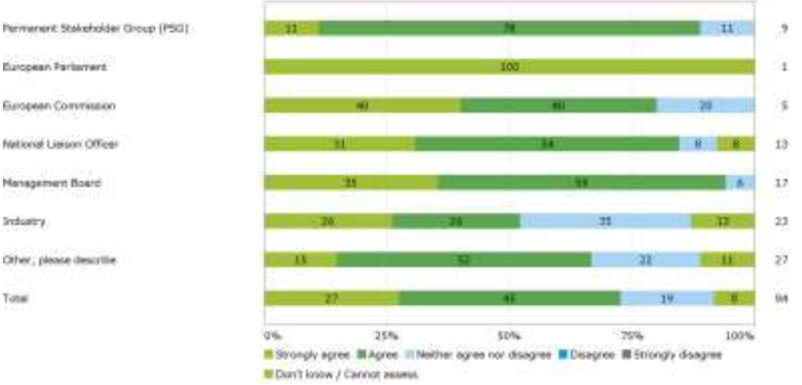


Figure 28: Q 2.5 The input provided by ENISA to implement new policies for NIS in the EU is useful

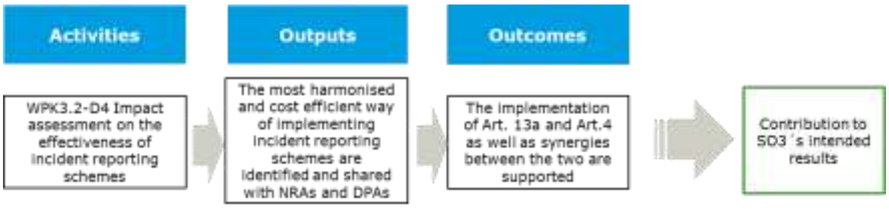


Please note that there were no interview findings which related specifically to this WPK – more general findings can be found in section 4.2.4.

4.2.4.2 Work Package 3.2: Assist EU Member States and Commission in the implementation of EU NIS regulations

WPK 3.2 aims at supporting EU Member State in implementing regulation, especially in the area of reporting according to Article 13a of the Telecoms Directive. The figure below provides an overview of which outputs and outcomes each deliverable under WPK 3.2 was intended to deliver in order to contribute to the achieving the intended results under SO3.

Figure 29: Simplified intervention logic for WPK 3.2



Activities

Outputs

Outcomes

WPK3.2-D4 Impact assessment on the effectiveness of incident reporting schemes

The most harmonised and cost efficient way of implementing incident reporting schemes are identified and shared with NRAs and DPAs

The implementation of Art. 13a and Art.4 as well as synergies between the two are supported

Contribution to SO3´s intended results

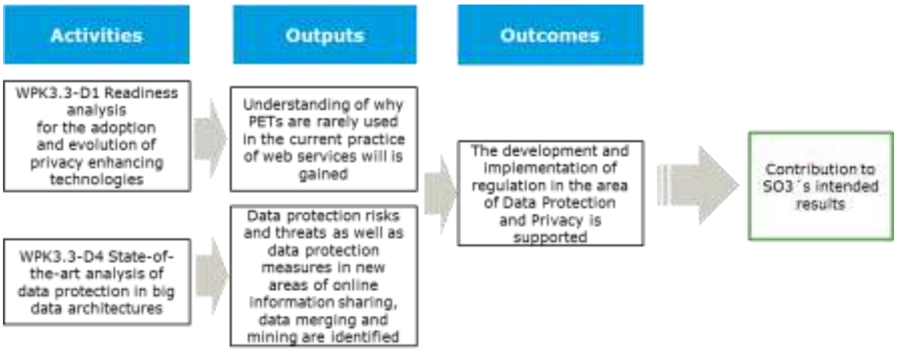
It is important to note in relation to the deliverable D4 "Impact assessment on the effectiveness of incident reporting schemes (e.g. Articles 13a and Art 4)" that the KII whereby "12 Member States make direct use of the outcomes of Article 13a work by explicitly referencing it or by adopting it at nationally level" had been achieved at the time of writing. In fact, as further presented in Appendix 4, 23 countries have implemented the Article 13a requirements, and on average 15 of them (more than 60%) declared that they have used different work produced by the group in their national implementation and work, providing concrete evidence of the impact that ENISA's work is having.

Please note that there were no interview or survey findings which related specifically to this WPK.

4.2.4.3 Work Package 3.3: Assist EU Member State and Commission in the implementation of NIS measures of EU data protection regulation

WPK 3.3 aims to strengthen the Agency´s efforts in the field of privacy and trust by providing analysis of the readiness of the industry, public and private sectors for the adoption and evolution of privacy technologies. In its approach, ENISA uses the WPK 3.3 activities to build a bridge between data protection legislation and the actual protection mechanisms. The figure below provides an overview of which outputs and outcomes each deliverable under WPK 3.3 was intended to deliver in order to contribute to the achieving the intended results under SO3.

Figure 30 Simplified intervention logic for WPK 3.3


Activities
Outputs
Outcomes
WPK3.3-D1 Readiness analysis for the adoption and evolution of privacy enhancing technologies
Understanding of why PETs are rarely used in the current practice of web services will is gained
The development and implementation of regulation in the area of Data Protection and Privacy is supported
Contribution to SO3´s intended results
WPK3.3-D4 State-of-the-art analysis of data protection in big data architectures
Data protection risks and threats as well as data protection measures in new areas of online information sharing, data merging and mining are identified

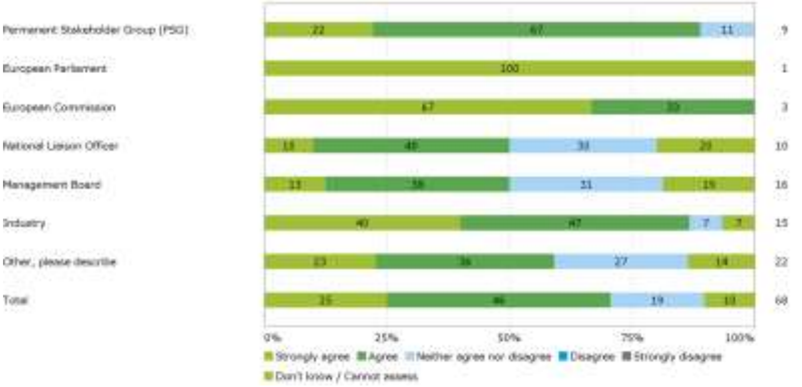
Approximately 30% of those surveyed had made use of the deliverables with a value of over EUR 30,000 which fall within this WPK, as the table below illustrates (a more detailed breakdown is presented in Appendix 5).

Table 8: Use made of given deliverables under WPK 3.3

Deliverable	Degree to which use was made of given deliverables (% that answered "Yes")
Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. Methodology, Pilot Assessment, and Continuity Plan	27%
Privacy By Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics	30%

The survey results further suggest that ENISA's activities support the development and implementation of Data Protection and Privacy regulation, with 71% of respondents either strongly agreeing (25%) or agreeing (46%) with this statement. Views among different types of stakeholders were relatively mixed, with NLOs and members of the Management Board rating this statement less positively / having less of an opinion than others, as the figure below illustrates.

Figure 31: Q 4.10 ENISA supports the development and implementation of Data Protection and Privacy regulation



This finding from the survey is also corroborated by the <u>case study</u> (for WPK 3.3), where the key finding was that the deliverable 4 under WPK 3.3 “Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics” made a strong contribution to supporting the implementation of Data Protection and Privacy regulation. This is in large part due to the fact that interviewees assessed that the publication provided concrete input to Data Protection Authorities (DPAs) on the challenges and possibilities of an increased focus on privacy in big data analysis, which was assessed to be primarily relevant in the context of implementation (and not development) of Data Protection and Privacy regulation. The target group interviewees were able to provide explanations and examples of how D4 has helped DPAs and private stakeholders understand, analyse and assess technical solutions from a legal or business perspective, and could confirm that this – already at an early stage- contributes positively to the implementation of the GDPR. This provides more tangible evidence showing that ENISA assisted stakeholders in Member States in implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security.

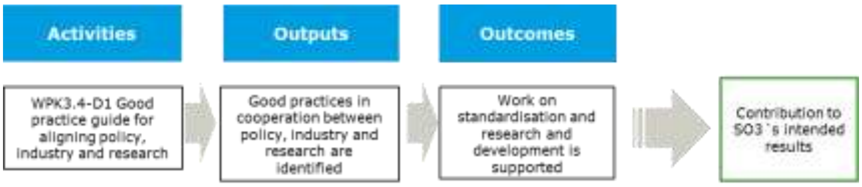
Further details on the case study findings and methodology can be found in a separate annex to this report.

Please note that there were no <u>interview</u> findings which related specifically to this WPK.

4.2.4.4 Work Package 3.4: RandD, Innovation and Standardisation

This WPK aims at supporting work on Standardisation (i.e. collaborating with standardisation bodies) and Research and Development (especially in the area of H2020). The figure below provides an overview of which outputs and outcomes each deliverable under WPK 3.4 was intended to deliver in order to contribute to the achieving the intended results under SO3.

Figure 32 Simplified intervention logic for WPK 3.4


Activities

Outputs

Outcomes

WPK3.4-D1 Good practice guide for aligning policy, industry and research

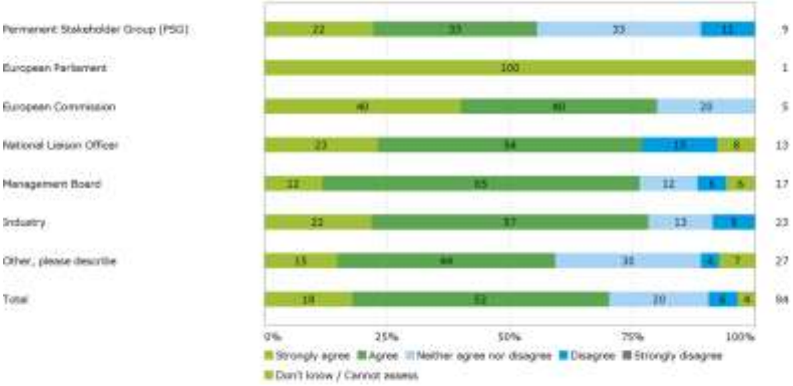
Good practices in cooperation between policy, industry and research are identified

Work on standardisation and research and development is supported

Contribution to SO3´s intended results

The survey results suggest that ENISA provides stakeholders with relevant information on standardisation, innovation and research, with 70% of stakeholders (strongly) agreeing with this statement, as the figure below further illustrates.

Figure 33: Q 2.6 ENISA provides stakeholders with relevant information on standardisation, innovation and research



Please note that there were no interview findings which related specifically to this WPK.

4.2.5 **Strategic objective 4**: To enhance cooperation both between the Member States of the EU and between related NIS stakeholders

ENISA's fourth strategic objective aims to enhance cooperation both between Member States of the EU and between related NIS stakeholders. It aims to do so by supporting EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS (WPK 4.1) and facilitating (WPK 4.2). The overall findings per data collection tool for SO2 and the findings in relation to each of its WPKs are presented below; the box below represents a conclusion in relation to SO2.

Conclusion on SO4

The evidence gathered in relation to SO4 suggests that in 2015 ENISA significantly enhanced cooperation both between Member States of the EU and between related NIS stakeholders. The survey findings point to the fact that the support from ENISA has contributed to a great extent to enhancing community building in Europe and beyond; increased the cooperation of operational communities; and improved services, workflow and communication among stakeholders to respond to crises. The interview results supported these findings, with stakeholders stressing the positive role that ENISA has in bringing people around the table to discuss and cooperate at an operational level. Key to this is the role that ENISA plays in supporting the sharing of information, ideas and common areas of interest among stakeholders. Finally, it was widely felt that ENISA's 2015 activities supported cooperation between stakeholders complements other public interventions, clearly pointing to a role for ENISA in this regard. However, there are areas for improvement as regards this SO in that the survey findings suggest that ENISA has enabled putting in place emergency mitigation and responses at low resources and time cost, and supported the development of technical capacity to a more limited extent.

Detailed findings per data source are presented below.

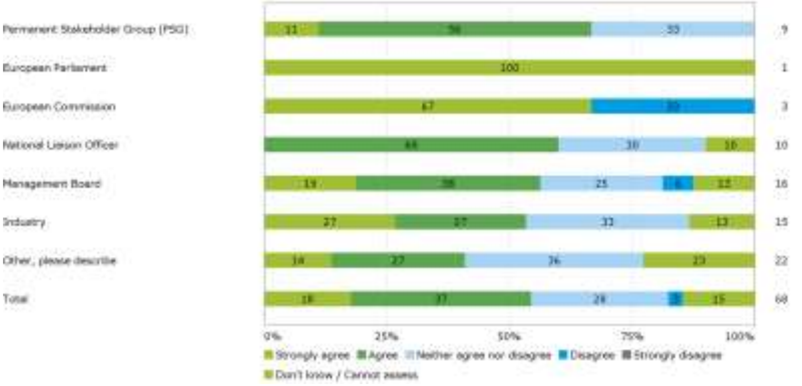
Survey findings

A total of 73% of survey respondents confirm that they are aware of ENISA's work to support cooperation between all relevant and active stakeholders in the area of NIS.[38] Overall, the answers provided in relation to this SO indicate that ENISA is currently effective at supporting cooperation.

In relation to the fourth SO's intended results, the survey findings suggest that:

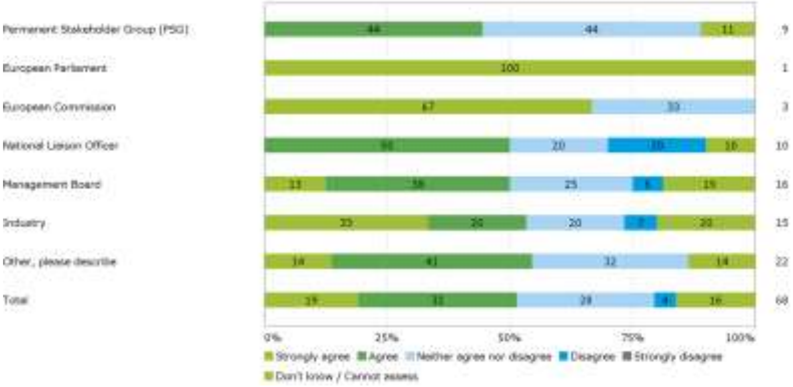
- The support from ENISA has strongly contributed to enhancing community building in Europe and beyond, with 85% of respondents (strongly) agreeing with this statement and no one disagreeing; see Appendix 5 for a breakdown by stakeholder type.
- ENISA's support has improved services, workflow and communication among stakeholders to respond to crises; 68% (very close to the 70%) were of this opinion and, once again, few disagreeing; see Appendix 5 for a breakdown by stakeholder type.
- ENISA's support enabled putting in place emergency mitigation and responses at low resources and time cost to a more limited extent, with only 54% of respondents (strongly) agreeing with this statement, as Figure 34 further illustrates.
- Technical capacity had increased among involved stakeholders to a more limited extent as well, with only 52% of those surveyed being of this opinion, as Figure 35 further illustrates. This result stands in contrast to that derived from last year's survey where 42% agreed with this statement.

Figure 34: Q 4.8 ENISA's support has enabled emergency mitigation and responses to be put in place at low resource and time costs



[38] Survey Question 4.1

Figure 35: Q 4.7 Technical capacity has increased among involved stakeholders



In-depth interviews

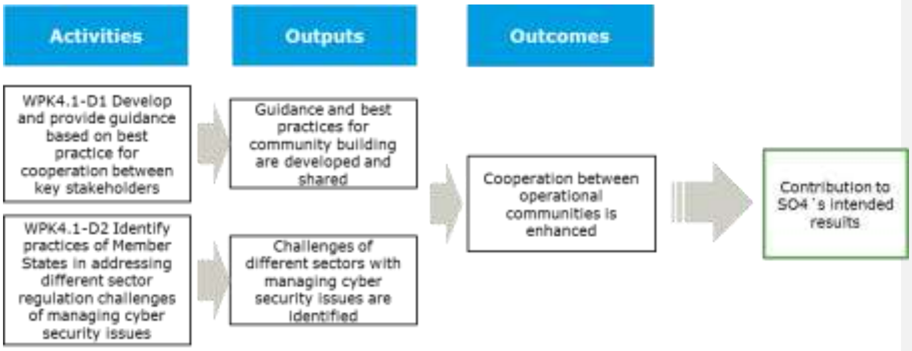
Representatives of the Management Board emphasised the positive role that ENISA had in bringing people around the table to discuss and cooperate at an operational level. For example, the cyber security exercise was assessed as an area where ENISA added value and succeeded in fostering cooperation between the EU and other NIS stakeholders. This view was shared by representatives of the PSG and the European Commission.

Generally the assessment of stakeholders on the extent to which ENISA´s 2015 activities contributed to cooperation between the Member States and between related NIS was positive. Both representatives of the Management Board and of the PSG who provided an assessment, indicated examples of actions of the 2015 activities fostered cooperation between Member States of the EU and between related NIS. In this sense, one representative of the PSG indicated that ENISA has engaged with the industry and provided the example of the Symantec state of Privacy Report to which ENISA contributed. Additionally, the example of Cyber Europe was provided to support the argument that ENISA has contributed to enhanced cooperation between Member States. However, further engagement and cooperation was deemed necessary by stakeholders**,** in particular representatives of the PSG.

4.2.5.1 Work Package 4.1: Support for EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS

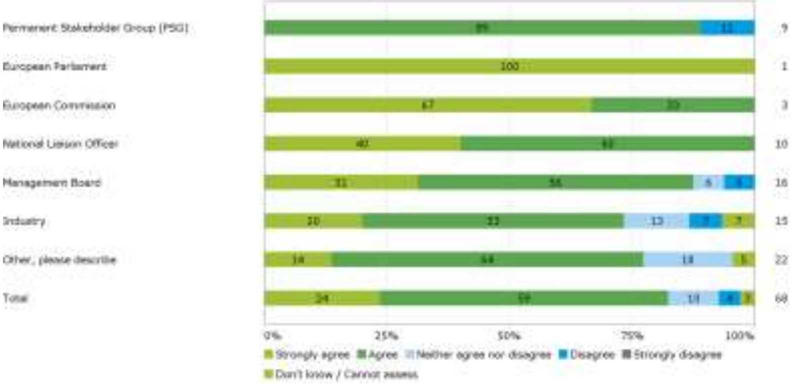
WPK 4.1 is intended to leverage the positive experience of ENISA in supporting CERTs, the CERT communities and Law Enforcement communities to come up with mutually satisfactorily ways to collaborate in NIS. The figure below provides an overview of which outputs and outcomes each deliverable under WPK 4.1 was intended to deliver in order to contribute to the achieving the intended results under SO4.

Figure 36 Simplified intervention logic for WPK 4.1


Activities
Outputs
Outcomes
WPK4.1-D1 Develop and provide guidance based on best practice for cooperation between key stakeholders
WPK4.1-D2 Identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues
Guidance and best practices for community building are developed and shared
Challenges of different sectors with managing cyber security issues are identified
Cooperation between operational communities is enhanced
Contribution to SO4´s intended results

A high proportion of respondents to the survey (82%) were of the opinion that ENISA's support has contributed to enhanced cooperation in operational communities; these positive views were shared by all stakeholder types (see Figure 37). This finding is strengthened by the fact that a wider stakeholder base was consulted in relation to this outcome this year and a lesser (though still significant) 70% of respondents were of this opinion last year.

Figure 37: Q 4.5 ENISA's support has contributed to enhanced cooperation in operational communities

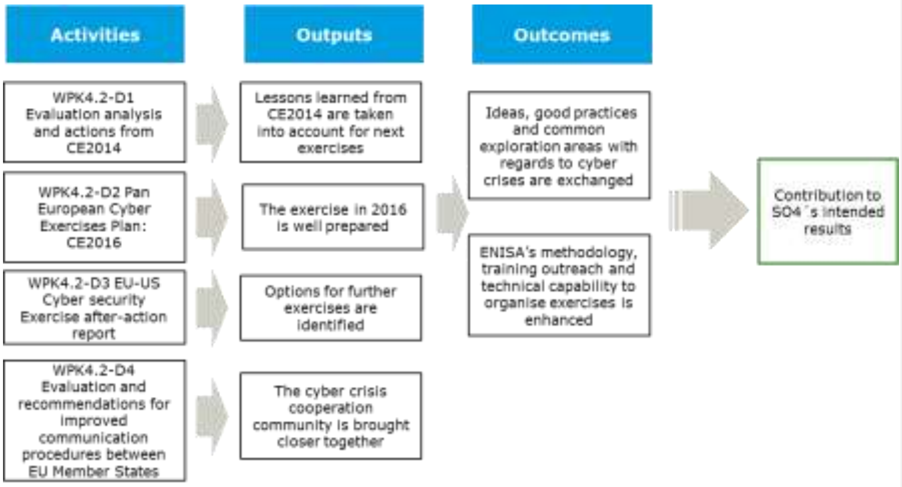


Please note that there were no interview findings which related specifically to this WPK.

4.2.5.2 Work Package 4.2: European cyber crisis cooperation through exercises

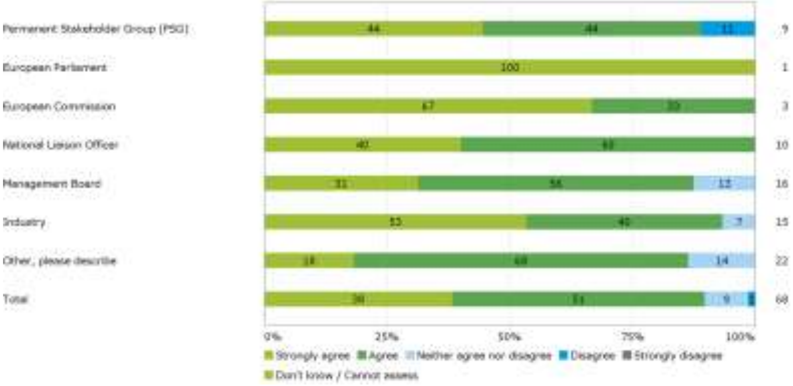
WPK 4.2 aims at facilitating the planning of the next pan European Cyber Exercise in 2015-2016. ENISA will further enhance its methodology, training outreach and technical capability to organise large-scale cyber crisis exercises. The figure below provides an overview of which outputs and outcomes each deliverable under WPK 4.2 was intended to deliver in order to contribute to the achieving the intended results under SO4.

Figure 38 Simplified intervention logic for WPK 4.2


Activities
Outputs
Outcomes
WPK4.2-D1 Evaluation analysis and actions from CE2014
WPK4.2-D2 Pan European Cyber Exercises Plan: CE2016
WPK4.2-D3 EU-US Cyber security Exercise after-action report
WPK4.2-D4 Evaluation and recommendations for improved communication procedures between EU Member States
Lessons learned from CE2014 are taken into account for next exercises
The exercise in 2016 is well prepared
Options for further exercises are identified
The cyber crisis cooperation community is brought closer together
Ideas, good practices and common exploration areas with regards to cyber crises are exchanged
ENISA's methodology, training outreach and technical capability to organise exercises is enhanced
Contribution to SO4´s intended results

A very high proportion of respondents to the survey (90%) were of the opinion that ENISA effectively supports the sharing of information, ideas and common areas of interest among stakeholders, with 38% of respondent strongly agreeing with this statement; these positive views were broadly shared by all stakeholder types, as the figure below illustrates.

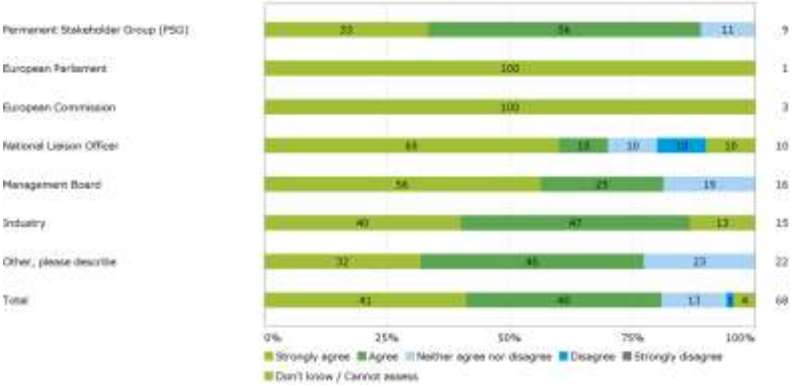
Figure 39: Q 4.2 ENISA effectively supports the sharing of information, ideas and common areas of interest among stakeholders



Moreover, 83% of survey respondents (excluding industry stakeholders) agree that ENISA's support to cooperation between stakeholders complements other public interventions; see Appendix 5, Q 4.3 for further details.

Finally, 81% of survey respondents agree that ENISA effectively shares lessons learned from cyber security exercises with other communities and sectors, as the figure below further illustrates.

Figure 40: Q 4.4 ENISA effectively shares lessons learned from cyber exercises with other communities and sectors



Please note that there were no interview findings which related specifically to this WPK.

4.3 Overall assessment of the efficiency of ENISA´s activities

Efficiency has been assessed based on the tracking of costs for deliverables (reports or other relevant units when applicable). Furthermore, the extent to which ENISA has cost saving measures in place, and how costs are followed up in the operations was assessed.

Conclusions on efficiency

On the basis of the evidence available, it can be concluded that ENISA´s 2015 activities were overall regarded as efficient, although the geographical location of the Agency and the split between Heraklion and Athens was assessed to reduce efficiency.

Generally, the evidence suggests that ENISA's processes are efficient and there is a clear delineation of responsibilities within the organisation, leading to a good execution of the work. In part this positive assessment relies on evidence that ENISA had some cost-saving measures in place during 2015, though some stakeholders suggested additional measures which could be put in place. It should be emphasised that the Agency has internalised a number of activities and reduced its usage of external resources and tendering, thus lowering costs. For example, Cyber Europe and CERT capacity building were highlighted as success stories (Cyber Europe being the number one success study and CERT capacity building the second), which were undertaken alone on the basis of internal expertise. In addition, the Agency continued to hire contract agents (as staff), rather than temporary agents during 2015, though this was also suggested to have its down-sides (see section 4.2.1 on effectiveness). Finally, only one case of low efficiency was identified, namely that the dissemination of ENISA´s publications during 2015 (and also more generally) could be improved. The evaluation assesses that this would be an efficient way of increasing the Agency´s effectiveness and boosting its impacts.

The evaluation also found that the operational budget of ENISA is limited, and the main expenditure relates to staff costs (similar to the findings presented in the 2014 evaluation). In the light of the resources available (staff and expenditures), ENISA manages to produce quite a high number of deliverables which also have generated considerable outreach in terms of downloads.

Please note that the cost per download was not assessed, since it is judged premature at this earlier point in the year to make such a calculation as many 2015 publications were only put *online in January of this year; such a calculation will be included in next year's report.*

Detailed findings per data source are presented below.

Desk research

The table below presents an overview of the cost of the deliverables under review as part of this evaluation, i.e. those with a value of over EUR 30,000. The deliverables under SO1 were the most costly comparatively speaking, which corroborates the views expressed by interviewees, that SO1 would require a significant degree of resources if more efforts were to be made in this vain in the future. Moreover, certain deliverables stand out as being more expensive than others including:

- WPK 2.1, D3: Maintaining CERT Good Practice and Training Library (Q4/2015) with a cost of over EUR 90,000;
- WPK 1.2, D1: Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3/2015) with a cost of over EUR 70,000;
- WPK 4.2, D2: Pan European Cyber Exercises Plan: CE2016 (restricted report, Q4 2015) with a cost of over EUR 70,000;
- WPK 4.1, D1: Develop and Provide Guidance Based on Best Practice for Cooperation Between Key Stakeholder Communities (Trust Building for and Reaching Out to New Communities) (CERTs, CIIP Community, Law Enforcement, Financial Services, Data Protection) (Q4//2015) with a cost of over EUR 70,000.

In last year's report, the cost per download was assessed, but it is judged premature at this earlier point in the year to make such a calculation as many 2015 publications were only put online in January of this year; such a calculation will be included in next year's report. That said, the data for 2014 core operational activities presented in last year's report has been updated on the basis of the additional analysis carried out on the web analytics (see Appendix 6 and Appendix 8) in order to establish a baseline against which judgements can be made year-on-year. The cost per download for the 2014 publications have been updated accordingly in Appendix 6.

Table 9: Overview of the cost of given 2015 deliverables

Strategic Objective	Workpackage	No	Deliverable title / report	Cost EUR
SO 1 To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS) Staff resources FTE 16,8[39]	WPK 1.1 NIS Threats Analysis	D1	Annual Threat Analysis / Landscape Report (Q4, 2015)	34,000
		D2	Risk Assessment on two emerging technology / application areas	54,897
	WPK 1.2 Improving the Protection of Critical Information Infrastructures	D1	Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3/2015)	77,882.94[40]
		D2	Methodology for the identification of Critical Communication Networks, Links, and Components (Q4/2015)	40,844
		D4	Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector (Q4/2015)	38,000
		D5	Good Practices and Recommendations on Resilience and Security of eHealth Infrastructures and Services	30,000 [41]

[39] Source: Annual Activity Report 2015

[40] WPK 1.2 D1 Cost of Printing Services not included (700 EUR)

[41] WPK 1.2 D5 Cost of Catering Coffee Breaks (435 EUR) and cost of Catering Lunch (1016,98 EUR) not included

Strategic Objective	Workpackage	No	Deliverable title / report	Cost EUR
	WPK 1.3 Securing Emerging Technologies and Services	D1	Good Practices and Recommendations on the Security and Resilience of Intelligent Transportation Systems (Q4/2015)	41,692.50[42]
		D2	Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4/2015)	32,000
		D3	Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4/2015)	41,662.50
TOTAL SO 1				**390,978.94**
SO 2 To assist MS and the Commission in enhancing capacity building through the EU Staff resources FTE 11,0[43]	WPK 2.1 Assist in Public Sector Capacity Building	D1	Support and Advise Member States on the Establishment and Evaluation of National Cyber Security Strategies (NCSS) (Q4/2015)	32,200[44]
		D3	Maintaining CERT Good Practice and Training Library (Q4/2015)	93,609
		D4	Building Upon the Evaluation Update ENISA's Methods in CERT Capacity Building and Propose a Roadmap (Q4/2015)	**Missing**[45]
		D5	Impact Evaluation on the Usefulness of the ENISA Guidelines on Capacty Building (Q4/2015)	49,294
Total SO 2				**175,103**
SO 3 To assist MS and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security Staff resources FTE 14,6[46]	WPK 3.1 Provide Information and Advice to Support Policy Development	D1 and D2 (Compiled)	Qualified Website Authentication Certificates. Promoting Consumer Trust in the Website Authentication Market	47,197.60
	WPK 3.2 Assist EU MS and Commission in the Implementation of EU NIS Regulations	D2	Recommendations on Addressing Root Causes of Specific incidents (report) (Q3/2015)	**Missing**[47]
		D4	Impact Assessment on the Effectiveness of Incident Reporting Schemes (e.g. Art13A and Art 4) (Q4/2015)	48,424
	WPK 3.3 Assist EU MS in the Implementation of NIS Measures of EU Data Protection Regulation	D1	Readiness analysis for the adoption and evolution of privacy enhancing technologies	30,000
		D4	State-of-the-art Analysis of Data Protection in Big Data Architecture	32,996.05
	WPK 3.4 R&D, Innovation & Standardisation	D1 and D2	Good Practice for Aligning Policy, Industry and Research (Q4/2015)	34,519.32
Total SO 3				**193,136.97**

[42] Cost of Catering Service not included (1471,5 EUR)
[43] Source: Annual Activity Report 2015
[44] WPK 2.1 D1 Cost of Printing Services (1935 EUR), cost of Catering Riga (3550 EUR), cost of Catering Latvia (7739,5 EUR) not included
[45] Data missing from budget information
[46] Source: Annual Activity Report
[47] Data missing from budget information

Strategic Objective	Workpackage	No	Deliverable title / report	Cost EUR
SO 4 To enhance cooperation both between MS of the EU and between NIS related communities **Staff resources FTE 10,6** [48]	WPK 4.1 Support for EU Cooperation Initiatives Amongst NIS-Related Communities in the Context of the EU CSS	D1	Develop and Provide Guidance Based on Best Practice for Cooperation Between Key Stakeholder Communities (Trust Building for and Reaching Out to New Communities) (CERTs, CIIP Community, Law Enforcement, Financial Services, Data Protection) (Q4//2015)	72,494 [49]
		D2	Identify Practices of Member States in Addressing Different Sector Regulation Challenges of Managing Cyber Security Issues (Q4/2015)	39,719
	WPK 4.2 European Cyber Crisis Cooperation Through Exercises	D1	Evaluation Analysis and Actions from CE2014 (restricted report, Q2, 2015)	24,332 [50]
		D2	Pan European Cyber Exercises Plan: CE2016 (restricted report, Q4 2015)	76,288 [51]
		D4	Evaluation and Recommendations for Improved Communication Procedures Between EU MSs (public / restricted report) (Q4, 2015)	**Missing**[52]
Total SO 4				**212,833**

Source: Annual Activity Report 2015 (draft)

In-depth interviews

In order to assess its efficiency, interviewees were asked whether ENISA had any cost saving measure in place.

Stakeholders of the PSG assessed that ENISA's processes are generally efficient and there is a clear delineation of responsibilities within the organisation. However, one representative of the industry indicated that there are certain discussions concerning ENISA's location, which constitutes a challenge in relation to its efficiency, but no further comments were provided in this regard. In terms of cost saving measures, it was indicated that ENISA could leverage the industry and involve stakeholders in projects. This could lead to cost reductions and burden sharing. Cross-transfer/mentoring from industry to ENISA staff could also be encouraged.

In a similar manner, representatives of the Management Board provided a generally positive assessment of ENISA's efficiency, while two of them pointed out certain difficulties concerning imposed on the efficiency of ENISA by its geographical location. It was further explained that the division between Heraklion and Athens is decreasing the efficiency of the management of activities and affects the visibility of its activities at EU level. In this regard, the use of video conferences for meetings (including those of the Management Board) was suggested by one stakeholder as a means to increase the frequency of meetings without increasing the need to travel and spend resources. At the same time, such measures are in use by the Agency.

One representative of the Management Board also suggested that ENISA's efficiency is actually increased through the internalisation of activities and the reduction of external resources and tendering. For example, Cyber Europe and CERT capacity building were provided as success

[48] Source: Annual Activity Report

[49] WPK 4.1 D1 Cost of Proofreading NSP Deliverable (290,1 EUR), cost of Proofreading CSIRT Maturity Report (470,6 EUR) not included

[50] WPK 4.2 D1 Cost of Printing Services (1530 EUR, cost of Commitment for Catering of CE2014 SLEX Event 24th-25th (10694,46 EUR), cost of C3E Rome Catering Services (7895 EUR) not included

[51] WPK 4.2 D2 Cost of C3E Workshop OCT Catering Services (6995 EUR), cost of Cyber Europe Branding Material (9595 EUR), cost of Printing Services (Posters and Stickers) CE2015 (700 EUR), cost of C3E Branding Material (3100 EUR), cost of Cyber Europe Exercises Stickers (326 EUR) not included

[52] Data missing from budget information

stories (Cyber Europe being the number one success study and CERT capacity building the second), which were done alone based on internal expertise. Thus, one of the cost saving methods suggested by one representative of the Management Board was to produce more internally and less through external tendering. One representative of the Management Board indicated that ENISA is doing comparatively well in terms of quality of output and that they value quality over quantity.

Another stakeholder of the Management Board indicated that ENISA is running efficiently despite limited budget. The limited budget determines ENISA to acquire contract agents, which are not as highly paid as temporary agent. The limited budget was assessed as being a challenge, in particular, in light of an increase in the tasks of ENISA.

Case studies

The case studies were intended to focus on the effectiveness of ENISA´s 2015 activities and therefore provided limited assessments of the efficiency of ENISA´s activities. This was also due to the fact that interviewees were not informed about the Agency´s budgets and the benefits derived from its activities. As mentioned in section 4.2.1, interviewees did highlight that further ENISA´s publications could deliver benefits to more stakeholders than is currently the case, and underlined that by improving its dissemination strategies, ENISA could boost effectiveness at a relatively low cost.

4.4 Coordination and coherence

An important aspect of ENISAs' work is the coordination and cooperation with involved stakeholders in NIS at the EU, Member State and international level.

Conclusions on coordination and coherence

Based on the evidence available, the evaluation finds that in 2015 ENISA actively pursued coordination with national and EU stakeholder including Europol, EC3, CERT EU, NIS platform at EC, PPP being launched by the EC, OSCE working group). In terms of potential gaps, only one (evident) gap in collaboration network was noted, namely with FRA, while the evidence also proposes that ENISA further improves cooperation with stakeholders in industry and academia.

Overall, the evaluation finds that sufficient coordination is carried out with relevant stakeholders, though the evidence available does not provide details on how the coordination is organised in more formal terms (apart from through the PSG and events such as the Annual Privacy Forum - APF).

In terms of ENISA´s general coherence with other national and EU level initiatives, the coordination (mentioned above) appears to pay off, and the evidence clearly shows that ENISA's 2015 deliverables to support NIS policy at the EU level complement those of other public interventions. No adverse effects of complementarity were identified, but the findings suggest a number of areas where there is room for improvement.

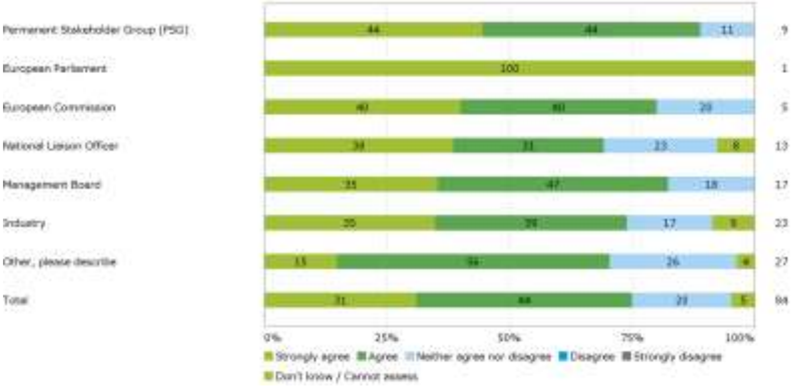
Overall, it can be concluded that ENISA's effectively cooperates and engages with its main stakeholders as stipulated in the mandate, and the evaluation findings are in line with those of the 2014 evaluation.

Detailed findings per data source are presented below.

Survey findings

A total of 75% of survey respondents agree that ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions, as further illustrated in the figure below.

Figure 41: Q2.3 ENISA’s deliverables to support NIS policy at the EU level complement those of other public interventions



In-depth interview results
In order to assess the coordination and coherence of ENISA with other bodies, a series of questions were asked of interviewees; and whether its activities contradict or complement the work of other public bodies.

First of all, **the views of stakeholders were generally positive on the extent to which ENISA coordinates activities with relevant bodies, offices and agencies in the field of Information and Communications Technologies (ICT)**, though more could be done in relation to certain stakeholders, while keeping in mind that this remains an area of Member State competence. This assessment relates to ENISA in general and is applicable to the activities during 2015.

The European Parliament representatives generally had a positive position towards the extent to which ENISA coordinates activities with other relevant bodies and offices. Additionally, it was noted that the EC understands better the role and importance of ENISA and that it would be expected that ENISA would have a better mandate and leverage. However, it was also mentioned by another EP representative that a more important focus on SMEs should be set. The assessment was shared by representatives of the European Commission. These comments appear to apply to the Agency more generally and are not exclusive to 2015.

The representatives of the PSG assessed that all relevant stakeholders are involved and consulted in the work of ENISA. Some exceptions, mentioned by one representative of the PSG, included NATO and other similar global/US organisations in Asia. Additionally, PSG representatives assessed positively their involvement in the work of ENISA and indicated that they were active in the work of the PSG, in Cyber Europe, in the Public Private Partnership on Cyber Security, and were involved in the evolution of discussions on data protection and the impact they have on cyber security. However, they also indicated that more efforts could be made in coordinating activities with the industry and engaging the industry further.

The assessment of Management Board representatives was generally positive in connection to the extent to which ENISA coordinates activities with relevant bodies, offices and agencies in the field of ICT. It was indicated that various stakeholders, including industry stakeholders are involved and that ENISA acts as a platform for cooperation and networking between various actors. However, it was also noted by two representatives of the Management Board that the involvement of the Member States varies to a large extent and that larger Member State are more involved in ENISA's activities. This is due to the unlike small Member States, large Member State have the capacity to keep up-to-speed with ENISA's activities. In this respect, it was suggested by one representative of the Management Board that an informal group of smaller Member State could be set up to exchange information and discuss problems of concern.

In addition to this, it was noted that private sector actors could be involved even more in ENISA's activities, e.g. strategy landscape papers – making sure to get information from a broad selection of sources is included which would increase the quality of the reporting even more.

However, overall, the opinion of some representatives of the Management Board was that in the coordination of actions on cyber security, the role of the Member State should remain central. In relation to this, it was suggested that one potential avenue for ENISA to be more active in coordination would be by more actively engaging the NLO network to invite the Member State in activities of ENISA and by providing Member States information in advance and relevant contact information with ENISA experts.

In a second instance, **the assessment of the extent to which ENISA's 2015 activities contradict or complement those of other public bodies offered a relatively mixed picture**. While some interviewees (in particular representatives of the Management Board) indicated that they were unaware of similar bodies that do similar work as ENISA, other representatives of the Management Board and the PSG indicated that some overlap does exist, in particular with:

- Europol (cybercrime dimension, incident reporting, disclosure of vulnerabilities, incident response),
- the NIS platform run by EC
- CERT EU
- EC3
- the PPP being launched by the EC,
- FIRST,
- OSCE (they have an informal working group that aims at building capacity in the field).

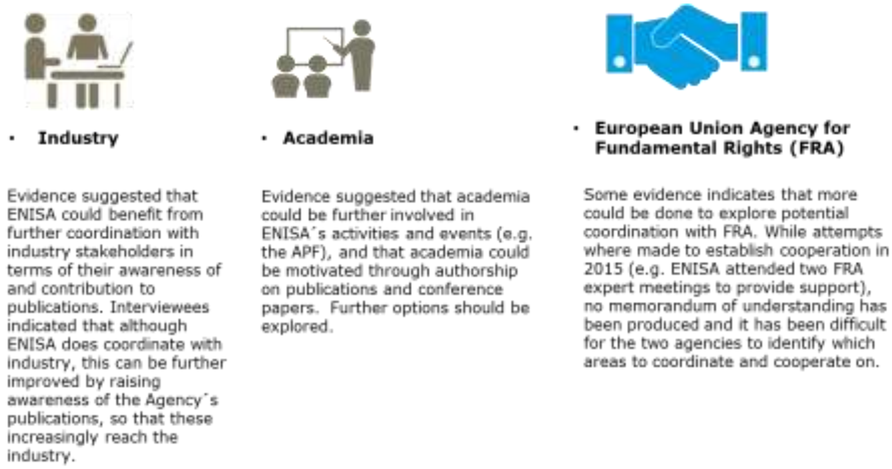
In terms of complementarity, all interviewees that provided an answer to this question acknowledged that, despite the fact that a certain extent of overlap exists, the actions of ENISA are also complementary with those of similar forums. Furthermore, one representative of the Management Board also indicated that a certain extent of overlap is reassuring as it confirms the importance of the issues and the accuracy of information provided by the different fora. The interviewees did not report any adverse or unintended effects of the overlap. One representative of the Management Board indicated that one of the unintended effects of overlap between ENISA and other agencies could be heightened awareness at political level of cyber security through assistance in development of strategy.

Case studies

The findings from the case studies generally highlighted that ENISA is very proactive in its involvement and coordination with relevant bodies, organisations and companies on EU and national level. This confirms the positive findings from the survey and the in-depth interviews. Similar to the findings from in-depth interviews, it is not clear how formalised ENISA´s coordinate with national and EU-level stakeholders.

The case studies suggested that ENISA could further improve its coordination and coherence in relation to industry, academia and FRA. It is important to note that the case studies generally assess ENISA´s coordinate and coherence with all relevant stakeholders as good.

Figure 42: Potential areas where coordinate and coherence can be improved



- **Industry**

Evidence suggested that ENISA could benefit from further coordination with industry stakeholders in terms of their awareness of and contribution to publications. Interviewees indicated that although ENISA does coordinate with industry, this can be further improved by raising awareness of the Agency´s publications, so that these increasingly reach the industry.

- **Academia**

Evidence suggested that academia could be further involved in ENISA´s activities and events (e.g. the APF), and that academia could be motivated through authorship on publications and conference papers. Further options should be explored.

- **European Union Agency for Fundamental Rights (FRA)**

Some evidence indicates that more could be done to explore potential coordination with FRA. While attempts where made to establish cooperation in 2015 (e.g. ENISA attended two FRA expert meetings to provide support), no memorandum of understanding has been produced and it has been difficult for the two agencies to identify which areas to coordinate and cooperate on.

The case studies did not identify any cases where the work of ENISA during 2015 contradicts that of other public intervention, though three interviewees highlighted that in relation to events (e.g. the APF), ENISA is in competition with many other similar conferences which take place, but that it could not be replaced by them. The case studies did not identify specific cases where ENISA´s work complemented those of other public interventions, but the findings do suggest that national administrations tended to focus on the 2015 ENISA activities which supported their own national priorities.

4.5 Overall assessment of the impact of ENISA´s activities

Impact concerns the extent to which ENISA's core operational activities contributed to reaching more long term and overall objectives. It should be kept in mind that in general terms, impact is only achieved after a certain amount of time, and is also highly or even mainly dependent on the environment and contextual factors. This is true in particular for policy agencies like ENISA, since the impact can only take place in the larger community by stakeholder applying and/or using ENISA's outputs.

Conclusion on impact

Based on the evidence available, it can be concluded that in 2015 ENISA made a contribution towards increased NIS in the EU, despite a limited mandate and resources. This finding is strong since a wide range of stakeholders have been consulted during this year´s evaluation.

The evidence shows that ENISA´s stakeholders assess that the Agency´s 2015 activities have contributed to ensuring a high level of NIS within the EU. This is a strong finding, underlining the impact of ENISA with respect to ensuring a high level of NIS. More specifically, the evidence shows that ENISA is key in developing a high level of NIS within the EU by fostering information sharing, providing technical expertise, enhancing the awareness of stakeholders to their own preparedness.

Moreover, the evidence clearly shows that the consulted stakeholders confirm that ENISA clearly contributed to raising awareness of NIS within the EU, and that the Agency has done so through its 2015 activities. In this regard, the evidence suggests that the activities that ENISA develops (e.g. Cyber Europe) were essential in enhancing the awareness of stakeholders of their own preparedness and developing the level of preparedness to cyber security.

Finally, ENISA´s stakeholders agree that ENISA promoted a broader culture of NIS in society during 2015. However, while evidence indicates the activities that ENISA develops to promote a culture of NIS in society, it is not possible for the evaluator to assess the extent to which the efforts of ENISA translate into practice, i.e. into actually building a culture of NIS in society.

Despite some shortcomings to the effectiveness of ENISA´s activities having been highlighted previously, it appears that the outcomes and results achieved by the Agency in 2015 have had a significant impact.

These findings are in line with those of the 2014 evaluation.

Detailed findings per data source are presented below.

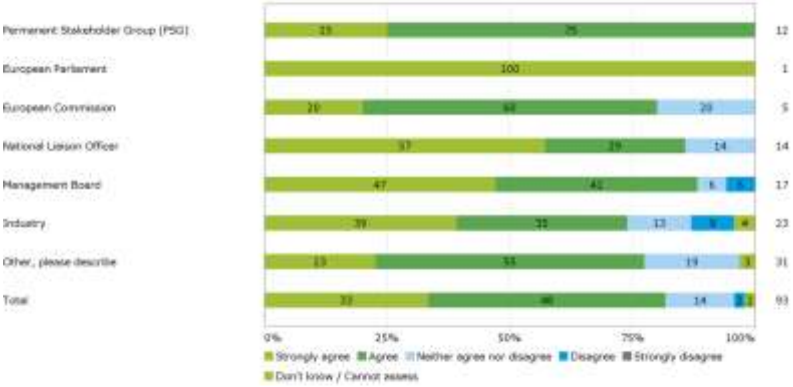
Survey findings

In the survey of stakeholders, questions were asked on whether ENISA has contributed to:

- ensuring a high level of NIS within the EU;
- raising awareness on NISA within the EU;
- promoting a culture of NIS within the EU.

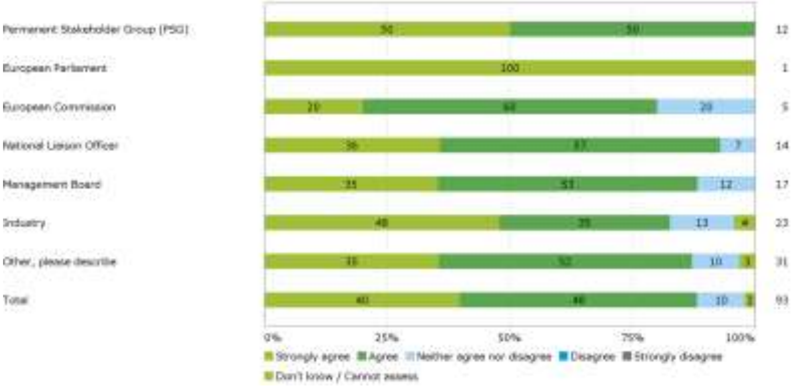
Results are positive with regards to the perceived impact of ENISA’s support. A total of 82% of respondents agree that ENISA contributes to ensuring a high level of NIS within the EU.

Figure 43: Q 5.1 ENISA clearly contributes to ensuring a high level of NIS within the EU



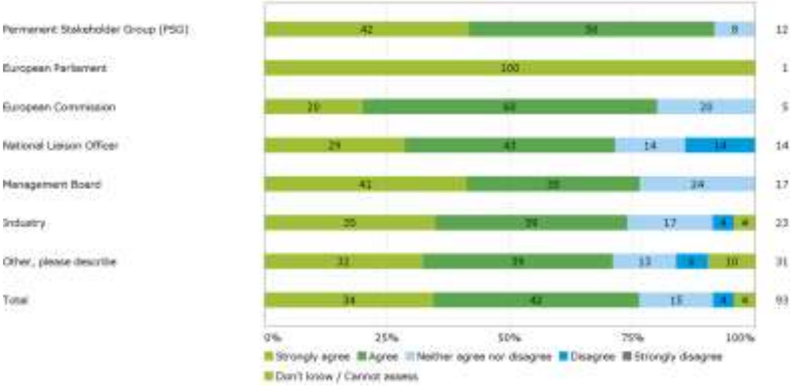
A further 88% of respondents confirm that ENISA clearly contributes to raising awareness of NIS within the EU.

Figure 44: Q 5.2 ENISA clearly contributes to raising awareness of NIS within the EU



In relation to promoting a broader culture of NIS in society, 76% of respondents agree that ENISA contributes to this.[53]

Figure 45: Q 5.3 ENISA contributes to promoting a culture of NIS in society



The survey results in relation to these three questions were comparatively high last year.

In-depth interviews

During the in-depth interviews, stakeholders were asked a series of questions in order to ascertain the extent to which ENISA's core operational activities contribute to achieving more long term objectives (impact), as set out in its legal act.

In a first instance, stakeholders were asked whether ENISA contributes to ensuring a high level of NIS within the EU, and what more could be done to this end. The European Parliament representatives assessed that **more could be done** in terms of solving the issue of location and funds. One representative of the EP indicated that ENISA's resources should be revisited and solutions were suggested including further involvement of the industry or further integration in H2020 activities dealing with cyber security. The representative of the EP even mentioned that a stronger role with stronger executing funding could enhance the visibility and contribution of ENISA to ensuring a high level of NIS.

[53] Survey Question 5.3

While assessing the contribution of ENISA positively, representatives of the PSG suggested that more could be done in terms of engaging with the institutions at EU level more and focusing on tangible outputs like incident reporting. The representative also indicated that the role of ENISA in terms of implementation of policies is relatively passive. At present, ENISA drafts reports with recommendations on certain issues which are transmitted to Member States. In this respect, more could be done on issues that are not contentious with Member States (e.g. skills, incident reporting) where the role of ENISA could be more practical in supporting and coordinating implementation. These assessments clearly related to the Agency´s activities in general and do not exclusively apply to its activities during 2015.

As regards representatives of the Management Board, the picture was more mixed. Various representatives of the Management Board acknowledged that the role of ENISA is key in developing a high level of NIS within the EU by fostering information sharing, providing technical expertise, enhancing the awareness of stakeholders to their own preparedness. However, one representative of the Management Board assessed that the level of expertise in the Member States is currently not high enough and gaps still exist in terms of understanding at political level and awareness in general to cyber security. The field is constantly evolving and it requires EU expertise and more resources in both government and private sectors, for investment and capacities. Additionally, another representative of the Management Board indicated that ENISA's mandate is relatively broad and that, in the future, the Agency should focus on areas which add the most value, e.g. expertise on specific technologies in spirit of subsidiarity.

The activities that ENISA undertakes (e.g. Cyber Europe) were assessed as essential in developing the level of preparedness to cyber security and enhancing the awareness of stakeholders of their own preparedness. Although ENISA is providing a high level or expertise, it was assessed that not all activities and deliverables during 2015 were supported or used by all Member States, due to the variegated perception of Member States in terms of their own preparedness and competence (e.g. in the discussion on cryptography in 2015 the perception on the added benefit of ENISA varied from one Member State to another). However, smaller Member States acknowledged the added value and benefits of the deliverables of ENISA, which were even used, in some cases, in the drafting of national strategies and implementation plans. The representatives of smaller states also indicated that ENISA is crucial for developing the NIS and developing a network to share information amongst states with similar resources. However, it was assessed that more could be done through facilitation of bilateral exchanges and work exchanges and developing sharing platforms which would proactively engage stakeholders. In addition to this, one representative of the Management Board even indicated that an informal group could be created for smaller nations to work together and find common ground on similar projects.

In a second instance, stakeholders were asked whether ENISA contributed to raising awareness on NIS, and what more could be done to this end. **Awareness raising on NIS is considered essential by most interviewees and the role of ENISA in this regard was assessed as pivotal**. One representative of the Management Board even indicated that currently there are numerous gaps in understanding of NIS at national level and the awareness of the general population is generally low. Furthermore, as cyber security is continuously evolving and it is a complex issue, awareness raising is important for all Member States alike. This assessment related to the ENISA´s activities in general and does not exclusively apply to its activities during 2015.

The EP advised that more can be done in terms of raising awareness on NIS, including increasing the visibility of ENISA reports through stronger marketing of reports, the organisation of events in Member State together with CERTS, leading and organising events with business and other partners, contributing to some research areas). Additionally, one representative of the EP indicated that one of the primary challenges in connection to raising awareness on NIS is constituted by the engagement of SMEs and suggested that ENISA should enhance its focus on them. This aspect was assessed as pivotal, in particular in countries with small companies that manage protection infrastructure.

According to one PSG representative, ENISA has contributed to a considerable extent to the raising awareness on NIS amongst policy-makers at EU level through conferences and seminars. However, at national level, the remit of its influence is limited by its mandate. The PSG representatives indicated that more could be done to amplify the message by using PSG members to increase awareness and by making the topics of discussion more specific, for example it could focus on running campaigns on given areas.

The members of the Management Board assessed that ENISA does contribute to a wide extent to awareness raising through its various activities, including those implemented in 2015. Two representatives of the Management Board mentioned as one of the main examples the contribution that ENISA had in the development of the European Month on Cyber Security and the cyber security quiz that had 25,000 subscribers. Another representative of the Management Board also highlighted the fact that ENISA has already developed a strategy on raising awareness and provides assistance in this regard (Article 12).

Finally, interviewees were asked whether ENISA contributes to promoting a culture of NIS in society. The **assessment of representatives of the PSG, the European Commission, the European Parliament and the Management Board was positive in relation to the activities that ENISA develops to promote a culture of NIS in society in general**. However, the interviewees were unable to assess the extent to which the efforts of ENISA translate into practice, i.e. into actually building a culture of NIS in society. It was noted by one representative of the PSG and one of the European Commission that the efforts of ENISA are in general focused more on the macro level of policy-makers and to a lesser extent on general population and industry. However, one representative of the Management Board assessed that the general population level was also the level where most "gaps" in understanding of the importance of cyber security exist.

The representatives of the Management Board also had a positive assessment of ENISA's contribution, but one of them indicated that more could be done by, for example, developing a generic awareness raising programme that could be used by Member States to inform relevant employees. This would be a credible way of doing more that would not overstretch the Agency resource-wise.

Case studies

The case studies did not investigate the overall impact of ENISA, but focused on the effectiveness on the 2015 activities (see section 4.2).

4.6 Overall assessment of the EU added value of ENISA’s activities

This section presents the evaluation´s findings on the extent to which ENISA´s 2015 activities have EU added value. This assessment is made by examining the extent to which:

- ENISA provides relevant and reliable information, trainings and exercises, which other national/international sources do not provide (scope effects).
- The Agency supports national actions in general (‘mirroring’) or specific areas of national policy (‘boosting’) (volume effects).
- Identification of cases where ENISA’s activities are coordinated or overlaps with other bilateral or European initiatives

Conclusion on EU added value
Based on the evidence available, there is moderate support to ENISA´s 2015 activities adding value overall and the findings are mixed.

On the one hand, the evidence does not pass the judgment criteria (from the evaluation matrix) in relation to whether ENISA has scope effects – in other words, evidence indicates that the information provided by ENISA is also in several cases provided by other sources. In addition to this, evidence suggests that ENISA´s 2015 activities had limited mirroring and volume effects – that is that ENISA´s activities do not support national actions in general or specific national actions to a satisfactory extent. Moreover, evidence showed that ENISA duplicates efforts because other similar initiatives are taking place. To some extent, this challenge is assessed to be due to the different needs of stakeholders, which mean that some ENISA activities are highly relevant while others are not.

On the other hand, evidence also showed that while many stakeholders acknowledged overlaps between ENISA´s 2015 activities and those of other national or EU institutions, they argued that this was in part compensated by ENISA´s activities being complementary – for example, as an independent source, they could be used for cross-checking information. In addition, evidence suggests that on an EU level, ENISA´s technical expertise is largely unique.

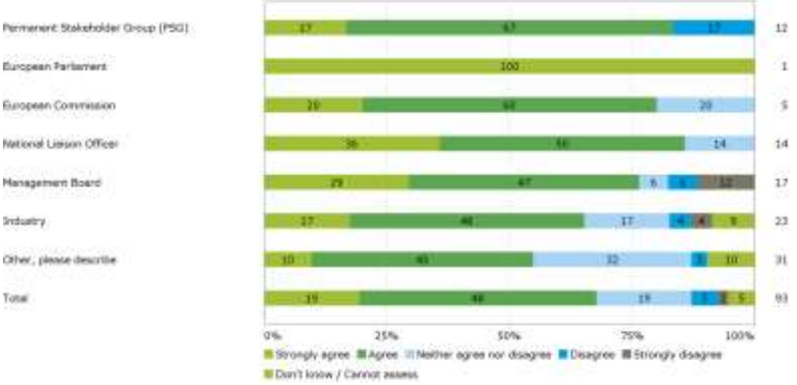
These findings are interesting since the shortcomings identified are not corroborated by findings from assessing the extent to which ENISA coordinates and ensures coherence with other bodies, organisations and the like. Therefore, the EU added value of ENISA´s activities should be investigated further, in particular focusing on examining concrete cases of overlaps to provide a more detailed assessment of cases where overlap has occurred, and how a duplication of efforts can be avoided.

Please note that EU added value was not assessed during the 2014 evaluation.

Detailed findings per data source are presented below.

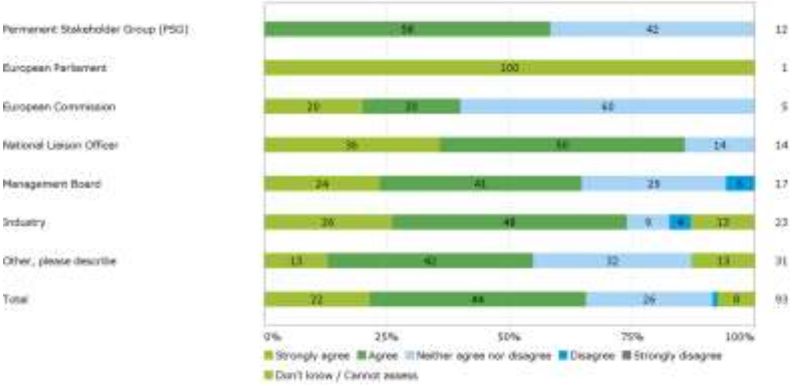
Survey findings
A total of 68% of respondents agree that ENISA contributes with relevant and reliable information, which other sources do not provide.

Figure 46: Q 6.1 ENISA contributes with relevant and reliable information, which other sources do not provide



Moreover, 66% of survey respondents agree that ENISA supports national actions in general[54], while 65% of respondents agree that ENISA supports specific areas of national action[55] (see Appendix 5).

Figure 47: Q 6.2 ENISA supports national actions in general

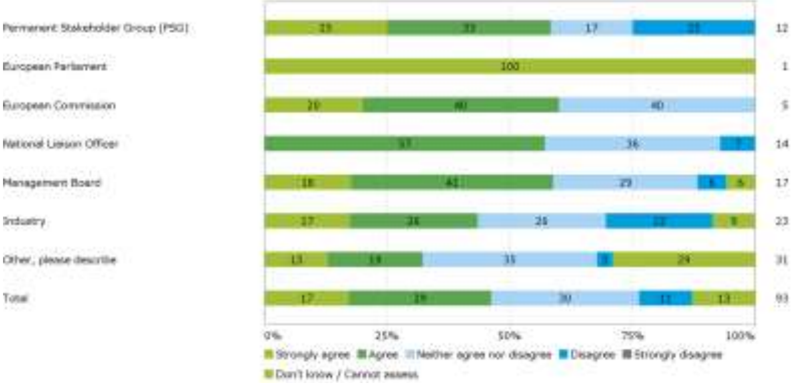


While respondents generally assess that ENISA provides stakeholders with relevant and reliable information, which other sources do not provide, nearly 46% also suggest that the Agency at times duplicates other efforts, and that not all stakeholders benefit equally.

[54] Survey Question 6.2

[55] Survey Question 6.3

Figure 48: Q 6.4 There are cases where ENISA activities duplicate efforts, because other similar initiatives are taking places



This is illustrated by a number of comments in the survey, including the one shown below.

> *"From a distant view, it seems that ENISA is centralised to particular issues and maybe a part of the stakeholders are left out, for example energy operators, retail markets and big industrial consumers".*

In-depth interview results

Stakeholders were asked a series of questions to assist in the assessment of the EU added value of ENISA and responded both in relation to the Agency in general as well as its activities during 2015. Please note that the European Parliament representatives did not provide an assessment of the added value of ENISA's work[56].

First of all, **the assessment of the representatives of the PSG, European Commission and the Management Board was generally positive in relation to the contribution of ENISA to reliable and relevant information that complements other sources and brings a governmental agency perspective on the matter of cyber security** The interviewees representing the PSG, European Commission and Management Board mentioned various sources that complement the information that ENISA provides including national sources, European Commission sources, Europol, OECD but also industry sources, such as SANS and FIRST. The representatives of the Management Board and the PSG noted that a certain amount of overlap with other sources does exist, but this was assessed by one Management Board representative as reassuring as it reinforces the accuracy and reliability of information.

Moreover, stakeholders were asked to assess whether the Agency supports national actions in general ('mirroring') or specific areas of national policy ('boosting'). According to the interviewed stakeholders, the added value of ENISA arises from the strong role in capacity building and advocating information security at EU level, and from the potential it presents in connecting the industry with policy makers at EU level. Additionally, it was stated by representatives of the Management Board that the Agency's support of national actions is pivotal in the development and implementation of European policies and in supporting technical experts at national level (e.g. Cyber Europe and CCERT/CSIRT network). However, one representative of the Management Board and one representative of the PSG also noted that the support of ENISA should be in line

[56] The availability of these interviewees was often limited, so a focus was placed on other aspects of the evaluati on instead.

with the subsidiarity principle and that a more operational response to incidents is better suited at national level and falls in the remit of competences of national actors. Additionally, one representative of the PSG further noted that further efforts could be made by ENISA to disseminate its deliverables.

Finally, interviewees were asked whether there were any cases where ENISA activities are coordinated or overlap (duplication of efforts) with other bilateral or European initiatives. Generally, the interviewed representatives of the PSG and Management Board reported that to a certain extent there is some **duplication of efforts** between the 2015 activities of ENISA and activities developed by other European institutions (e.g. Europol). However, the interviewed representatives also indicated that the work of ENISA is to a large extent unique and complements the work of other institutions. However, more work could be done in terms of aligning the activities of ENISA with those of the industry (for example Future Cyber Security Private-Public Partnership).

In terms of coordination, various stakeholders reported instances of **coordination between ENISA and national level stakeholders** were reported. For example the representative of the Management Board for Ireland reported coordination between the defence forces of Ireland and ENISA on the Cyber Europe exercise). Additionally, a representative of the PSG also reported instances of coordination with ENISA on the threat analysis report and cloud analysis report where efforts were made by ENISA to include stakeholders.

Case studies

The case studies were designed to focus on the effectiveness of ENISA´s 2015 activities and did not examine their EU added value.

5. CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the conclusions and recommendations for the evaluation of ENISA´s 2015 activities. It is structured in six sections and each one is dedicated to one of the six evaluation criteria. These sections present concise answers to the evaluations questions and the evaluation´s key conclusions and recommendations for a given criteria.

5.1 Relevance

The table below presents the three evaluation questions related to “relevance” and provides a concise answer to each of them based on the indicators, judgement criteria and data sources, as included in the evaluation matrix (see Appendix 1).

Table 10 Answers to evaluation questions - Relevance

Evaluation Question	Answer (in summary)[57]
To what extent are the core operational activities carried out in line with ENISA’s legal mandate?	The evaluation did not identify any cases where a task was carried out without legal base. Majority of tasks in Article 3.1 are addressed
To what extent do the core operational activities carried out correspond to the actual needs of the stakeholders?	ENISA´s activities during 2015 clearly responded to the needs of a variety of stakeholders. ENISA’s work is seen as relevant to responding to the needs, and ENISA’s work and outputs are judged to be responding to a need for NIS across the EU and within Member States. ENISA was further judged to be effectively meeting its stakeholders’ expectations.
To what extent do the actual results achieved correspond to the needs of the stakeholders? (Utility)	The results derived from ENISA´s activities generally respond to the needs of stakeholders. In this regard, the evaluation found that some result were more relevant to given types of stakeholders than to others (for example because they corresponded to priorities in Member States).

Based on the answers to the evaluation questions and the findings presented in section 4.1, the evaluation has identified some key achievements and key challenges of ENISA. These are presented in the table below and represent areas where the Agency can improve or should maintain its relevance.

Table 11 Key conclusions and recommendations -Relevance

Conclusion	Recommendation
Ensuring a high level of NIS[58]: The evaluation findings confirm that at present cyber security threats are not being adequately addressed in the EU or at the national level in Member States. ENISA´s core operational activities are shown to be contributing to addressing this gap by supporting the EU and Member States in their efforts to increase NIS. Whether the actual results of activities have met the needs is more difficult to ascertain. Hence it will be important for ENISA to further prioritise its efforts in areas with greatest needs and/or where least attention is being paid to the NIS threats.	As stated, the need for improved NIS in Europe is far greater than what ENISA can provide with its current remit and available resources. It will therefore be important for the Agency to focus on the right priorities based on what the most pressing needs are and where it has the legal mandate to support and has the capacity and resources to provide high quality input. Currently ENISA is aiming to, and mostly succeeds in, accommodating the needs and wishes from a diverse range of stakeholders, thereby striking a good balance (see conclusion “Supporting differing needs” below).

[57] Answers are provided in accordance with the indicators, judgement criteria and data sources set out in the evaluation matrix (see annex 1).

[58] See section 4.1 for the detailed analysis.

	However, by doing so, the Agency also *risks* dispersing already scarce resources across too many, too small activities, decreasing the chance of overall real impact on NIS It is recommended that ENISA elaborate a framework or methodology for a needs assessment to systematically map and prioritise its work, and act as a guide for the strategic planning of the Agency and the development of Annual Work Programmes. Such a framework would help ENISA and key stakeholders make the "hard choices" and focus efforts where they are most needed. The framework should be discussed and agreed in consultation with key stakeholders, and in particular the Management Board and PSG. At a higher level, this also reflects the fact that ENISA´s mandate is broad and that it should be considered whether all the objectives in the current mandate are equally important/relevant or if there is potential to reduce the scope of its mandate as part of future plans to revise it.
Supporting differing needs[59]: Currently ENISA strikes a balance in how it provides support to Member States depending on their needs and situation. 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 NCSS), while Member States with higher NIS capacity tend to benefit from technical studies, and contribute with best practices.	The Agency should (continue to) be aware of and take into account such differing needs in the work it carries out, e.g. by clustering Member States that have similar needs or objectives. This may seem to contradict the earlier recommendation on prioritisation, but it should be emphasised that prioritisations should be done on the basis of objectives, NIS weaknesses etc. and mot MS or stakeholders.

5.2 Effectiveness

The table below shows the four evaluation questions related to "effectiveness" and provides concise answers to each of them, based on the indicators, judgement criteria and data sources included in the evaluation matrix (see Appendix 1). It should be noted that questions relating to effectiveness have mainly been assessed on the basis of the evaluation of the core operational activities of 2015, as per the terms of reference and proposal for the assignment (see the M&E framework in Appendix 3).

Table 12 Answers to evaluation questions -Effectiveness

Evaluation Question	Answer (in summary)[60]
To what extent does ENISA achieve its objectives, as stipulated in the legal mandate?	Overall, 53% of the indicators (16 out of 30) (from the M&E framework) were achieved. This picture is also supported by the findings in relation to the degree of achievement of the KIIs (17 out of 28 to date). The legal mandate of ENISA is broad, and while the Agency attempts to address all tasks, not all are equally targeted. Within the NIS community there is a high diversity, between sectors as well as between Member States, which makes is difficult to achieve the ambitious objectives of ENISA.

[59] See section 4.1 for the detailed analysis.

[60] Answers are provided in accordance with the indicators, judgement criteria and data sources set out in the evaluation matrix (see Appendix 1).

To what extent are there areas for improvement?	The evaluation pointed to a number of key areas for improvement, including in relation to the Agency´s technical expertise in the area of emerging technologies, and ENISA´s opportunities to develop and exploit synergies with other stakeholders (in particular national CERTs).
To what extent is ENISA's organisation conducive to supporting the achievement of objectives?	The Agency´s organisation is overall conducive to supporting the achievement of objectives, and it is clear that the ENISA leadership manages the limited resources and capacities available very well. Even so, the understaffing and the difficulty to recruit the right expertise or sufficient level of seniority makes the Agency quite vulnerable and could potentially have an impact on the productivity and quality in the longer term.
To what extent are ENISA's systems and procedures conducive to supporting the achievement of objectives?	In general, it appears that planning and implementation of activities functions well. However, in relation to follow-up, the evaluation noted some shortcomings, namely the lack of detail in the evaluation forms for trainings, and limited data on the publications. This also meant that several KIIs could only be partially accessed, because data was missing. The evaluation found that that the quality management is sufficient and that deliverables are of high quality. The evaluation did not find any evidence suggesting that ENISA´s management lacked information to make informed decisions.

Based on the answers to the evaluation questions and the findings presented in section 4.2, the evaluation provides six key conclusions and recommendations. These are presented in the table below and either represent areas where the Agency can improve or should maintain its effectiveness.

Table 13 Key conclusions and recommendations - Effectiveness

Conclusion	Recommendation
Organisational set-up, processes and stakeholder involvement[61]: ENISA´s organisational set-up, processes and procedures support the Agency in involving stakeholders, executing its activities and thereby reaching its objectives. At the same time, some factors are restricting ENISA´s effectiveness, in particular the limited resources the Agency disposes of, the informal nature of the NLO network, not consistently crediting authors on publications, and the need to improve the dissemination of publications. In relation to the NLO network in particular, it appears to be making a limited contribution to ENISA´s work; this represents a challenge, in particular since NLOs appear to only rarely disseminate publications to national stakeholders.	Notwithstanding an increase in budget and expert staff, ENISA can improve its effectiveness by continuing to involve external experts in conducting technical studies, and motivate them in doing so by ensuring that authors are consistently credited (including on the front page). ENISA could increase the effectiveness of its publications by further disseminating them, thus reaching a broader audience. In this respect, it is recommended that the NLO network be incentivised to further disseminate ENISA's publications to national stakeholders.
Development of expertise[62]: While ENISA is contributing to the development and maintenance of a high level of expertise of EU actors (SO1), it is doing so to a limited extent. ENISA is considered a "trusted partner" by stakeholders, providing "relevant", "useful", "quality" inputs and advice. However, evidence	ENISA could consider lessening its focus on this more technical SO and invest more resources on a limited number of deliverables which provide the most added value / impact. This would make sense considering the expert resources needed to truly add value in this field, Member State's (CSIRT) competence and

[61] See section 4.2.1 for the detailed analysis.

[62] See section 4.2.2 for the detailed analysis.

points to the fact that ENISA's 2015 activities have not led to a significant increase in technical capacity, the promotion of relevant methods towards emerging technologies, or enabled opportunities for new technologies and approaches to a high degree. It is worthy of note that this is an objective which is most challenging to fulfil due to Member State (CSIRT) competence and capabilities in this more operational area; ENISA's more strategic mandate; and the limited resources at ENISA's disposal. Moreover, increasing technical capacity among stakeholders will take time to achieve; in many cases it proved too early to judge whether ENISA's 2015 activities have contributed to this long-term objective.	capabilities in this more operational area, ENISA's more strategic mandate, and ENISA's limited budget. In the future, a needs assessment could be undertaken with key experts to ascertain what the most important needs are.
Building capacity in the EU[63]***:*** ENISA has managed to enhance capacity building to a significant extent (SO2), but to varying degrees according to the stakeholder type. ENISA has assisted in enhancing the capacity of Member States (most notably smaller Member States) in particular through: the pivotal role it plays in bringing different actors together and building networks; the dissemination of good practices; the organisation of training sessions on a technical level; and its work on NCSS. However, more work needs to be done as cyber security challenges are not being as adequately addressed as they could be by Member States and in the EU; it is unclear what the role of ENISA is in relation to building the EU institutions' capabilities; and more could be done in relation to the private sector where ENISA remains relatively little known. This was also highlighted under the conclusions and recommendations for relevance above, showing that the Agency is addressing a real need for technical capacity building, but that further and continuous efforts are required.	In the future, more of a focus could be placed on building capacity within the EU institutions (including the Commission - see recommendation below), as well as increasing awareness of ENISA's work, and thereby further build capacity among private sector actors. The role of ENISA vis à vis the EU institutions could be examined in more detail during the evaluation which is scheduled to take place in 2017.
Supporting the development and implementation of policy[64]***:*** ENISA is more effective at supporting the *implementation* than the *development* of the policies necessary to meet the legal and regulatory requirements of NIS (SO3). ENISA's key contribution to the *implementation* of policies related to NIS resides in its thorough	Though potentially difficult due to resource constraints and the Commission and Member States' perceptions of ENISA's supportive (rather than central) role in the development of policies related to NIS, it may be beneficial to involve the Agency in the development of policies related to NIS through more coordination with the Commission and Member

[63] See section 4.2.3 for the detailed analysis.

[64] See section 4.4.2 for the detailed analysis.

understanding of the legal basis, the technical context, and stakeholders' views, however it plays a lesser role in the *development* of policies.	States. This would allow ENISA to ensure a consistent approach to cyber security across the various sectors concerned by given policy/legislative developments, such as the NIS directive. For example, it could look to be aware of the activities of and/or take part in working groups on cyber security issues set up by different Commission DGs from the outset.
Supporting cooperation in the EU[65]***:*** ENISA has significantly enhanced cooperation both between Member States of the EU and between related NIS stakeholders (SO4) by bringing people from different operational communities around the table to share information, ideas and common areas of interest at an operational level. ENISA has thereby contributed to a great extent to enhancing community building in Europe and beyond and improved services, workflow and communication among stakeholders to respond to crises. Moreover, it was widely felt that ENISA's support to cooperation between stakeholders complements other public interventions, clearly pointing to a role for ENISA in this regard. However, areas where ENISA could do more include: facilitating putting in place emergency mitigation and responses at low resources and time cost, as well as supporting the development of technical capacity, which it was seen to be doing to a more limited extent.	The first recommendation above, presented in relation to the findings concerning ENISA's SO1, is also applicable here.

5.3 Impact

The table below presents the evaluation question related to "impact" and provides a concise answer to it based on the indicators, judgement criteria and data sources, as included in the evaluation matrix (it can be found in Appendix 3).

As the answers to the evaluation questions show, it appears that the outcomes and results achieved by the Agency in 2015 have had a significant impact, despite some shortcomings to the effectiveness of ENISA´s activities having been highlighted previously.

Table 14 Answers to evaluation questions - Impact

Evaluation Question	Answer (in summary)[66]
To what extent do ENISA's core operational activities contribute to achieving more long term objectives (impact)?	A majority (82%) of survey respondents agree that ENISA contributed to *ensuring a high level of NIS within the EU*, with 40% of these strongly agreeing. This is a strong finding underlining the impact of ENISA with respect to ensuring a high level of NIS. The evaluation finds that ENISA is key in developing a high level of NIS within the EU by fostering information sharing, providing technical expertise, enhancing the awareness of stakeholders to their own preparedness.
	A majority (88%) of survey respondents confirm that ENISA clearly contributed

[65] See section 4.2.5 for further details.

[66] Answers are provided in accordance with the indicators, judgement criteria and data sources set out in the evaluation matrix (see Appendix 1).

	to *raising awareness of NIS within the EU*. In general, the activities that ENISA develops (e.g. Cyber Europe) have been important in enhancing the awareness of stakeholders of their own preparedness and developing the level of preparedness to cyber security.
	A majority (76%) of survey respondents agree that ENISA *promoted a broader culture of NIS in society.* The evaluation finds that the activities that ENISA develops to promote a culture of NIS in society. However, it was not possible to assess the extent to which the efforts of ENISA translate into practice, i.e. into actually building a culture of NIS in society

Based on the answers to the evaluation questions and the findings presented in section 4.5, evaluation provides three key conclusions and recommendations. These are presented in the table below and either represent areas where the Agency can improve or should maintain its impact.

Table 15 Key conclusions and recommendations -Impact

Conclusion	**Recommendation**
Ensuring a high-level of NIS[67]***:*** The evaluation found that ENISA makes an important contribution to ensuring a high level of NIS in the EU, but also indicates that more could be done in terms of further engaging with the institutions at EU level and focusing on tangible outputs like incident reporting.	It is recommended that the Agency focus on the areas which deliver the highest impact (as previously touched upon in the recommendation on relevance). These areas are suggested to be: providing expertise on specific technologies, including methodologies on how to assess the technologies advantages/disadvantages; events (in particular the Annual Privacy Forum - APF); and exercises (in particular the Cyber Europe exercise) where stakeholders network and learn from each other. The evaluation tentatively finds that the most successful deliverables (such as these) are those which are relevant to a large group of stakeholders, and demand high level expertise, which can be sourced both from ENISA (in particular in terms of coordination) and external contributors (with high level expertise).
Raising awareness of NIS[68]***:*** The evaluation found that awareness raising on NIS is considered essential by most stakeholders and the role of ENISA in this regard was assessed as pivotal. The findings indicated that some improvements could be made.	In order to further increase its impact on awareness raising, it is recommended that ENISA: • Improve its collaboration with NLOs, in particular by clarifying their role and scoping their tasks. • Continue implementation of its awareness raising capacity. • Improve effective dissemination of publications (through NLOs, its website,

[67] See section 4.5 for the detailed analysis.

[68] See section 4.5 for the detailed analysis.

	social media - in particular LinkedIn which appears to be used by different categories of stakeholders).
Achievement of impact[69] For ENISA, measuring impact is highly challenging and to a large extent dependent on contextual factors. 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 are more ambitious and provide a better starting point to measure ENISA´s contribution to reaching the impacts described above. However, it should be noted that the actual data needed to measure the KIIs does not appear to be available. 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.	It is 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. 5 years. It is 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. With regard to the latter, we have redesigned ENISA´s evaluation form to be used after events and trainings. In addition, we have developed a new follow-up form (to gather data on how new skills or knowledge impacts the users work) and an online survey (to follow-up on the usage of publications). It is recommended that such forms be used systematically in the future in order to assist ENISA in assessing the impact of an event/training session/publication. Using these forms will help to provide data to measure the KIIs. Other means of follow-up would need to be devised in relation to other types of activities.

5.4 Efficiency

The table below presents the two evaluation questions related to "efficiency" and provides concise answers to them based on the indicators, judgement criteria and data sources, as included in the evaluation matrix (it can be found in Appendix 1).

Table 16 Answers to evaluation questions - Efficiency

Evaluation Question	Answer (in summary)[70]
To what extent are the objectives achieved at a reasonable cost?	The cost per download was assessed, but it is judged premature at this earlier point in the year to make such a calculation as many 2015 publications were only put online in January of this year; such a calculation will be included in next year's report. A majority of stakeholders interviewed assessed that ENISA's processes are generally efficient and there is a clear delineation of responsibilities within the organisation.

[69] See section 4.2.1 for further details.

[70] Answers are provided in accordance with the indicators, judgement criteria and data sources set out in the evaluation matrix (see annex Appendix 1).

To what extent does ENISA have cost saving measures in place?	Stakeholders assessed that ENISA has some cost-saving measures in place, although they also suggested additional measures to be put in place. Stakeholders highlighted that the Agency has internalised a number of activities and reduced of external resources and tendering. For example, Cyber Europe and CERT capacity building were provided as success stories (Cyber Europe being the number one success study and CERT capacity building the second), which were done based on internal expertise.

Based on the answers to the evaluation questions and the findings presented in section 4.1, the evaluation provides two key conclusions and recommendations. These are presented in the table below and either represent areas where the Agency can improve or should maintain its efficiency.

Table 17 Key conclusions and recommendations -Efficiency

Conclusion	Recommendation
Organisational set-up and processes: ENISA generally functions efficiently; it is characterised by a clear delineation of responsibilities and has cost-saving measures in place, but one case of low efficiency was identified, namely the insufficient dissemination of publications.	By boosting its dissemination of publications, ENISA would be increasing its cost-effectiveness, since more stakeholders could benefit from the publications. As shown above, improved efforts from the NLO network could be one tenant in achieving this at a reasonable cost.
Difficulty in recruiting the expert staff[71]: The evaluation found that, in 2015, ENISA continued to struggle with hiring expert staff due to the salaries it can offer and its geographical location. Under the efficiency criteria it was also noted that the Agency used contract staff in 2015 (rather than temporary staff) to lower salary costs. This was suggested to be a key challenge for ENISA in terms of the Agency´s effectiveness.	Notwithstanding a budgetary increase and other factors changing, it is recommended that, in terms of cost saving measures, ENISA leverage the industry and involve them in projects. This could lead to cost reductions and burden sharing. Cross-transfer/mentoring from industry to ENISA staff and could also be encouraged – although no feasible options for how to implement such an initiative were identified.

5.5 Coordination and coherence

The table below presents the two evaluation questions related to “coordination and coherence” and provides concise answers to each of them based on the indicators, judgement criteria and data sources, as included in the evaluation matrix (it can be found in Appendix 1).

Table 18 Answers to evaluation questions – Coordination and coherence

Evaluation Question	Answer (in summary)[72]
To what extent does ENISA coordinate activities with relevant bodies, offices and agencies in the field of Information and Communications Technologies (ICT)?	Findings show that ENISA cooperates with relevant bodies, offices and agencies (Europol, EC3, CERT EU, NIS platform at EC, PPP being launched by the EC, OSCE working group) and only one (evident) gap in collaboration network was noted, namely with FRA. Overall, interviewees assess that sufficient coordination is carried out with relevant stakeholders, although they found it difficult to explain to how the coordination is organised in more formal terms (apart from through the PSG and events such as the APF).
To what extent does ENISA's activities contradict or complement	A majority (75%) of survey respondents agreed that ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions.

[71] See section 4.3 for the detailed analysis.

[72] Answers are provided in accordance with the indicators, judgement criteria and data sources set out in the evaluation (see Appendix 1).

those of other public interventions?	No adverse effects of complementarity were identified, but the findings suggest a number of areas where there is room for improvement.

Based on the answers to the evaluation questions and the findings presented in section 4.4, the evaluation provides one key conclusion and recommendation. These are presented in the table below and represent areas where the Agency can improve or should maintain its coordination and coherence.

Table 19 Key conclusions and recommendations – Coordination and coherence

Conclusion	Recommendation
Good coordination with other stakeholders: The evaluation shows that ENISA coordinates activities with relevant bodies, offices and agencies in the field of Information and Communications Technologies (ICT), though more could be done to align activities with other stakeholders in industry, academia and FRA, while keeping in mind that this remains an area of MS competence.	It is recommended that ENISA increase its coordination with private sector stakeholders, as well as increase their involvement in its activities (for example Future Cyber Security Private-Public Partnerships). Amongst EU bodies, ENISA´s expertise is largely unique, and its technical advice has potential to make an important contribution to other EU bodies, such as FRA as was seen when cooperation between the two agencies was explored during 2015. Other examples include Europol and EU-LISA.

5.6 EU added value

The table below presents the evaluation question and provides a concise answer to it based on the indicators, judgement criteria and data sources, as included in the evaluation matrix (it can be found in Appendix 1).

Table 20 Answers to evaluation questions – EU added value

Evaluation Question	Answer (in summary)[73]
What is the added value of ENISA?	A majority (68%) of survey respondents agree that ENISA contributes with relevant and reliable information, which other sources do not provide. A majority (66%) of survey respondents agree that ENISA supports national actions in general, while 65% of respondents agree that ENISA supports specific areas of national action. A minority (46%) of survey respondents agree that there are cases where ENISA duplicates efforts, because other similar initiatives are taking place. Despite the fact that a certain extent of overlap exists, the actions of ENISA are also complementary with those of similar forums. ENISA provides technical expertise which is unique amongst the EU institutions and agencies. No significant overlaps between Agency´s activities and other bilateral or European initiatives were identified, but the majority of stakeholders interview acknowledged that a certain extent of overlap exists between ENISA and bilateral or EU initiatives. At the same time the actions of ENISA are also complementary with those of similar forums (see section 5.5. above).

[73] Answers are provided in accordance with the indicators, judgement criteria and data sources set out in the evaluation matrix (see Appendix 1).

Based on the answers to the evaluation questions and the findings presented in section 4.6, the evaluation provides two key conclusions and recommendations. These are presented in the table below and represent areas where the Agency can improve or should maintain its EU added value.

Table 21 Key conclusions and recommendations – EU added value

Conclusion	**Recommendation**
Support to national policies*:* ENISA is to some extent appreciated for its support to national actions in the area of NIS in general (‘mirroring’), and its support to specific areas of national policy (‘boosting’), but appreciation does not appear to be as widespread as it could be.	It should be examined further to what extent any lesser level of appreciation can be explained by the fact that different stakeholders have different needs, for example while for some Member States ENISA’s work in a given area is already taking place at national level and therefore does not add value, the same work in this area may be useful to another Member State.
Duplication of efforts*:* It is assessed that there are cases where ENISA’s 2015 activities have duplicated the efforts of national and EU level stakeholders, and where the information provided by the Agency was provided by other sources. Such instances will reduce efficiency, and limit ENISA´s effectiveness. At the same time, it should be noted that ENISA’s 2015 activities provided EU added value, because the Agency has a strong role in capacity building and advocating information security at EU level, and supports Member States in implementing EU policies. Moreover, ENISA provides unique technical expertise at an EU level.	A more careful examination of cases where ENISA´s work overlaps or duplicates the work of other EU or national level stakeholders should be undertaken to ascertain when and with which organisations overlap occurs; how a duplication of efforts can be avoided; and which justifications there may be for multiple sources providing the same information (e.g. complementary information, ensuring an independent source of information, providing timely information or similar).

6. ACTION PLAN

The following table summarises the findings per evaluation criteria and outlines tentative actions for ENISA to consider.

Table 22: Action plan

Criteria	Summary findings	Possible Actions
Relevance Ensuring a high level of NIS	At present cyber security threats are not being adequately addressed in the EU or at the national levels in Member States. ENISA´s core operational activities in 2015 are shown to contributing to addressing this gap by supporting the EU and Member States in their efforts to increase NIS. Whether the actual results of activities have met the needs is more difficult to ascertain. Hence it will be important for ENISA to further prioritise its efforts in areas with greatest needs and/or where least attention is being paid to the NIS threats.	Continue to explore ways to ensure ENISA's work is addressing real needs in NIS in the EU. Elaborate a framework or methodology for a needs assessment in consultation with key stakeholders, and in particular the Management Board and PSG.
Relevance Supporting differing needs	Currently ENISA strikes a balance in how it provides support to Member States depending on their needs and situation. 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 NCSS), while Member States with higher NIS capacity tend to benefit from technical studies, and contribute with best practices.	Continue to be aware of and take into account that ENISA meets the needs of a diverse group of stakeholders.
Effectiveness Organisational set-up, processes and stakeholder involvement	ENISA´s organisational set-up, processes and procedures support the Agency in involving stakeholders, executing its activities and thereby reach its objectives. At the same time, some factors are restricting ENISA´s effectiveness, in particular the limited resources the Agency disposes of, the informal nature of the NLO network, not consistently crediting authors on publications and need to improve dissemination of publications. In relation to the NLO network, it appears to be making a limited contribution to ENISA´s work; this represents a challenge, in particular since NLOs appear to only rarely disseminate publications to national stakeholders.	Continue to involve external experts in conducting technical studies, and motivate them in doing so by ensuring that authors are consistently credited. Improve dissemination of publications, thus reaching a broader audience. Incentivise the NLO network to further disseminate ENISA's publications to national stakeholders.
Effectiveness Development of expertise	While ENISA is contributing to the development and maintenance of a high level of expertise of EU actors (SO1), it is doing so to a limited extent. ENISA is considered a "trusted partner" by stakeholders, providing "relevant", "useful", "quality" inputs and advice. However, evidence points to the fact that ENISA's activities in 2015 have not led to a significant increase in technical capacity (though this is an ambitious objective for an Agency with limited resources and in many cases it proved too early to judge whether ENISA's 2015 activities have contributed to such a long-term objective); the promotion of	Consider lessening its focus on this more technical SO and invest more resources on a limited number of deliverables which provide the most added value / impact. Consider undertaking a needs assessment with key experts to ascertain what the most important needs are.

Criteria	Summary findings	Possible Actions
	relevant methods towards emerging technologies; or enabled opportunities for new technologies and approaches to a high degree.	
Effectiveness Building capacity in the EU	ENISA has managed to enhance capacity building to a significant extent (SO2) in 2015, but to varying degrees according to the stakeholder type. ENISA has assisted in enhancing the capacity of Member States (most notably smaller Member States) in particular through: the pivotal role it plays in bringing different actors together and building networks; the dissemination of good practices; the organisation of training sessions on a technical level; and its work on NCSS. However, more work needs to be done as cyber security challenges are not being as adequately addressed as they could be by Member States and in the EU; it is unclear what the role of ENISA is in relation to building the EU institutions' capabilities; and more could be done in relation to the private sector where ENISA remains relatively little known. This was also highlighted under the conclusions and recommendations for relevance above, showing that the Agency is addressing a real need for technical capacity building, but that further and continuous efforts are needed.	Consider whether more of a focus could be placed on building capacity within the EU institutions (including the Commission - see recommendation below), as well as increasing awareness of ENISA's work, and thereby further build capacity among private sector actors. Examine the role of ENISA vis à vis the EU institutions in more detail during the evaluation which is scheduled to take place in 2017.
Effectiveness Supporting the development and implementation of policy	ENISA was judged more effective at supporting the *implementation* than the *development* of the policies necessary to meet the legal and regulatory requirements of NIS (SO3) in 2015. ENISA's key contribution to the *implementation* of policies related to NIS is the Agency´s thorough understanding of the legal basis, the technical context, and stakeholders' views, but it plays a lesser role in the *development* of policies.	Raise awareness of the fact that it may be beneficial for other EU institutions to increase their involvement of the Agency in the development of policies related to NIS. Highlight that ENISA can ensure a more consistent approach to cyber security across the various sectors concerned by given policy/legislative developments.
Effectiveness Supporting cooperation in the EU	ENISA significantly enhanced cooperation both between Member States of the EU and between related NIS stakeholders (SO4) in 2015 by bringing people from different operational communities around the table to share information, ideas and common areas of interest at an operational level. ENISA thereby contributed to a great extent to enhancing community building in Europe and beyond and improved services, workflow and communication among stakeholders to respond to crises. Moreover, it was widely felt that ENISA's support to cooperation between stakeholders complemented other public interventions, clearly pointing to a role for ENISA in this regard.	Continue to explore ways to ensure ENISA's work is addressing real needs in NIS in the EU.
Impact	The evaluation found that ENISA made an important contribution to ensuring a high level	Focus on the areas which deliver the highest impact (as

Criteria	Summary findings	Possible Actions
Ensuring a high-level of NIS	of NIS in the EU in 2015, but also indicated that more could be done in terms of further engaging with the institutions at EU level and focusing on tangible outputs like incident reporting.	previously touched upon in the recommendation on relevance), such as: expertise on specific technologies including methodologies on how to assess the technologies advantages/disadvantages; events (in particular the Annual Privacy Forum - APF); and exercises (in particular the Cyber Europe exercise) where stakeholders network and learn from each other.
Impact Raising awareness of NIS	The evaluation found that raising awareness on NIS is considered essential by most stakeholders and the role of ENISA in this regard was assessed as pivotal. The findings indicated that some improvements could be made.	Improve its collaboration with NLOs, in particular by clarifying their role and scoping their tasks. Improve effective dissemination of publications (through NLOs, website, social media - in particular LinkedIn which appears to be used by different categories of stakeholders).
Impact Achievement of impact	For ENISA, measuring impact is highly challenging and to a large extent dependent on the environment and contextual factors. Moreover, impact can often only really be judged over the longer term. In this respect, ENISA´s annual KIIs are an essential data source when it comes to monitoring the Agency´s impact over time. However, while the 2015 KIIs are the most ambitious so far, many still seek to ascertain "use" are more operational, focussing more on outputs (e.g. number of participants in a workshop) rather than actual contribution to an impact (e.g. using ENISA´s recommendations in national strategies). Moreover, actual data needed to measure the KIIs does not always appear to be available.	Set up a monitoring system which seeks to measure performance over a period of time (rather than annually) against pre-defined KIIs. Ensure that the KIIs capture impact rather that output. Improve the collection of data, by using new data collection tools (such as does redesigned or developed by the evaluator).
Efficiency Organisational set-up and processes:	ENISA generally functions efficiently; it is characterised by a clear delineation of responsibilities and has cost-saving measures in place, but one case of low efficiency was identified in 2015, namely the insufficient dissemination of publications.	Increase efficiency by improving dissemination of publications, since more stakeholders could benefit from the publications.
Efficiency Difficulty in recruiting the expert staff	In 2015, ENISA continued to struggle with hiring expert staff due to the salaries and the Agency´s geographical location. It was also noted that the Agency used contract staff (rather than temporary staff) to lower salary costs in 2015. This was suggested to be a key challenge for ENISA in terms of the Agency´s effectiveness.	Leverage the industry and involve industry stakeholders in projects. This could lead to cost reductions and burden sharing. Cross-transfer/mentoring from industry to ENISA staff and could also be encouraged.
Coordination and coherence	In 2015, ENISA coordinated activities with relevant bodies, offices and agencies in the	Increase coordination with and involvement of private

Criteria	Summary findings	Possible Actions
Good coordination with other stakeholders	field of Information and Communications Technologies (ICT), though more could be done to align activities with other stakeholders in the industry, academia and FRA, while keeping in mind that this remains an area of MS competence.	sector stakeholders. Continue to explore and push for cooperation with other EU level stakeholders, including FRA, Europol, EU-Lisa.
EU added value Support to national policies	In 2015, ENISA was to some extent appreciated for its support to national actions in the area of NIS general ('mirroring'), and its support to specific areas of national policy ('boosting'), but appears to not be as appreciated as it could have been.	Further examine to what extent ENISA supports national policies being developed and/or implemented, and why there are lesser levels of appreciation.
EU added value Duplication of efforts	It was assessed that there were cases where ENISA's 2015 activities duplicated the efforts of national and EU level stakeholders, and where the information provided by the Agency was also provided by other sources. Such instances will reduce efficiency, and limit ENISA´s effectiveness. At the same time, it should be noted that ENISA's 2015 activities provided EU added value, because the Agency has a strong role in capacity building and advocating information security at EU level, and supports Member States in implementing EU policies. Moreover, ENISA provides unique technical expertise on an EU level.	Carefully examine cases where ENISA´s work overlaps or duplicates the work of other EU or national level stakeholders to ascertain when and with which organisations overlap occurs, how a duplication of efforts can be avoided, and which justifications there may be for multiple sources providing the same information (e.g. complementary information, ensuring an independent source of information, providing timely information or similar). This could be done in the context of the evaluation scheduled tpo be carried out in 2017.

APPENDIX 1
EVALUATION MATRIX

In order to meet the requirements of generating robust findings over the entire period of the external evaluations, we have developed a two tier evaluation framework, one overall framework to be applied to all years being evaluated (evaluation questions matrix) and one more detailed framework targeting the core operational activities for each year (2015 in this instance).

An evaluation questions (EQ) matrix is a tool used to structure an evaluation by specifying the questions to be addressed, indicators to be used, judgement criteria and data sources. In this way, the EQ matrix serves to ensure that findings are solid, robust and transparent.

The EQ matrix below should thus be considered to cover all the years which can (potentially) be evaluated. It contains questions related to the evaluation criteria listed in the figure above (e.g. effectiveness, relevance, etc.). It should be noted that questions relating to effectiveness in particular, will mainly be based on the evaluation of the core operational activities of the year in question, as per the terms of reference for the assignment. This is further specified in the monitoring and evaluation framework developed for 2015, see Appendix 3.

As agreed at the kick off meeting for the 2015 evaluation, the evaluation question matrix has been extended to now also assess the EU added value of ENISA. This is a key evaluative criterion of the Commission’s Better Regulation guidelines. The assessment builds on the terms of the study which specify the need to assess the added value of the core operational activities, and ensure that a sufficient focus is put on the added benefits of approaching NIS at EU level, including the principles of subsidiarity and proportionality.

Table 23 Evaluation Matrix

Evaluation Question	Indicators	Judgement criteria	Data sources
Relevance			
To what extent are the core operational activities carried out in line with ENISA's legal mandate?	Degree of linkage between core operational activities and mandate Balance in addressing all tasks	No task carried out without legal base Majority of tasks in article 3.1 are addressed	Desk review
To what extent do the core operational activities carried out correspond to the actual needs of the stakeholders?	Stakeholders' are of the opinion that the core operational activities are responding to their needs	70% agree	Stakeholder survey Interviews with stakeholders
To what extent do the actual results achieved correspond to the needs of the stakeholders? (Utility)	Stakeholders' are of the opinion that the outputs from the core operational activities are responding to their needs	70% agree	Stakeholder survey Interviews with stakeholders
Effectiveness			
To what extent does ENISA achieve its objectives, as stipulated in the legal mandate?	High degree of achievements of objectives – as per specific M&E framework (yearly adapted to core operational activities)	Overall achievement 70% agreement in stakeholder surveys Overall assessment in interviews positive, with tangible examples of achievements provided	See M&E framework
To what extent are there areas for improvement?	Areas for improvement identified in implementation of core operational activities	N/A	Interviews with stakeholders
To what extent is ENISA's organisation conducive to supporting the achievement of objectives?	Cooperation and collaboration between departments functioning well Staff agree that ENISA's organisation is fit for purpose/supports the implementation of activities	Majority of interviewees agree	Interviews (Management Board)
To what extent are ENISA's systems and procedures conducive to support the achievement of objectives?	Project cycle well-functioning (planning, implementation, follow-up) Quality management system in place and used Management has relevant information available to make informed decisions	Majority of interviewees agree	Case studies[74]
Impact			

[74] We will look at this as part of the case studies while keeping with their primary focus to look at the implementation of the 2015 COAs.

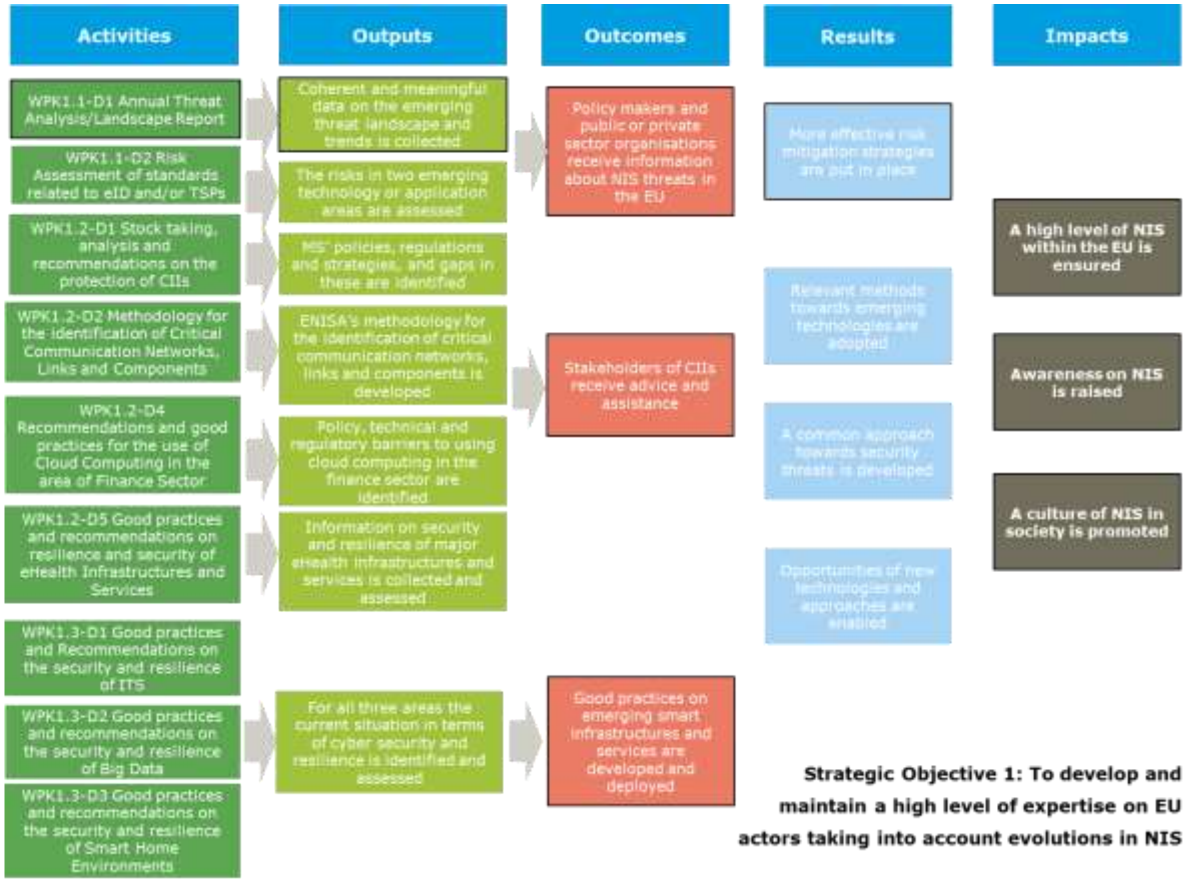
Evaluation Question	Indicators	Judgement criteria	Data sources
To what extent do ENISA's core operational activities contribute to achieving more long term objectives (impact)?	A high level of NIS within the EU is ensured	At least 70% of evaluation/survey respondents are of the opinion that ENISA contributes to ensuring that a high level of NIS within the EU Staff/stakeholders interviewed are of the opinion that ENISA contributes to ensuring that a high level of NIS within the EU, and provide concrete examples	Yearly stakeholder surveys Interviews with stakeholders
	Awareness on NIS is raised	At least 70% of evaluation/survey respondents are of the opinion that ENISA contributes to raising awareness on NIS Staff/stakeholders interviewed are of the opinion that ENISA contributes to raising awareness on NIS, and provide concrete examples	Yearly stakeholder surveys Interviews with stakeholders
	A culture of NIS in society is promoted	At least 70% of evaluation/survey respondents are of the opinion that ENISA contributes to promoting a culture of NIS in society Staff/stakeholders interviewed are of the opinion that ENISA contributes to promoting a culture of NIS in society, and provide concrete examples	Yearly stakeholder surveys Interviews with stakeholders
Efficiency			
To what extent are the objectives achieved at a reasonable cost?	Tracking of cost/resources used per deliverable Cost per download for reports	Stable costs Differences justifiable	ENISA's records
To what extent does ENISA have cost saving measures in place?	Cost saving measures in place Follow-up on costs	Continuous work/processes in place to save costs in the operations Follow-up measures in place	Interviews (Management Board)
Coordination and coherence			
To what extent does ENISA coordinate activities with relevant bodies, offices and agencies in the field of Information and	Collaboration networks in place in relevant field Coordination activities carried out	No (evident) gaps in collaboration network Sufficient coordination is carried out with relevant stakeholders	Yearly stakeholder surveys Interviews with stakeholders

Evaluation Question	Indicators	Judgement criteria	Data sources
Communications Technologies (ICT)?			
To what extent does ENISA's activities contradict or complement those of other public interventions?	View of other public stakeholders on ENISA's complementarity with other public interventions Any adverse effects from ENISA's work	At least 70% of evaluation/survey respondents are of the opinion that ENISA complements other public interventions No adverse effects identified	Yearly stakeholder surveys Interviews with stakeholders
EU-added value			
What is the added value of ENISA?	Stakeholder assessment of the extent to which ENISA provides relevant and reliable information, trainings and exercises, which other national/international sources do not provide (scope effects). Share of stakeholders stating that the Agency (1) supports national actions in general ('mirroring') or specific areas of national policy ('boosting') (volume effects). Identification of cases where ENISA's activities are coordinated or overlaps with other bilateral or European initiatives	At least 70 % of stakeholders assess that ENISA provides information which other sources do not. At least 70 % of stakeholders agree that the Agency supports national actions in general OR that it has supported specific areas of national policy. No significant overlaps between Agency activities and other bilateral or European initiatives.	Survey Interviews with stakeholders Case studies

APPENDIX 2
INTERVENTION LOGICS

Following on from the approach taken for the 2014 evaluation, ENISA’s intervention logics (ILs) have been updated based on the new strategic objectives for 2015. An intervention logic serves to illustrate how an intervention or activity is intended to work by showing the hierarchy of objectives and how one achievements should lead to another. In general, the higher level objectives are long term and cannot be controlled. The changes from the work streams in 2014 to the strategic objectives in 2015 have been marked in the intervention logic diagrams. All components which have stayed the same since 2014 are framed in black. The mapping shows that a number of outcomes and results[75] have stayed the same but that some changes have been made which have to be taken into account in the evaluation. These changes were taken into account in the design of the M&E framework presented in the subsequent annex, and by extension this evaluation.

[75] Outcomes refer to short term effects of an activity, for example dissemination of a report, whereas results refer to medium term effects, such as stakeholders actually using the report.



Activities

WPK1.1-D1 Annual Threat Analysis/Landscape Report

WPK1.1-D2 Risk Assessment of standards related to eID and/or TSPs

WPK1.2-D1 Stock taking, analysis and recommendations on the protection of CIIs

WPK1.2-D2 Methodology for the identification of Critical Communication Networks, Links and Components

WPK1.2-D4 Recommendations and good practices for the use of Cloud Computing in the area of Finance Sector

WPK1.2-D5 Good practices and recommendations on resilience and security of eHealth Infrastructures and Services

WPK1.3-D1 Good practices and Recommendations on the security and resilience of ITS

WPK1.3-D2 Good practices and recommendations on the security and resilience of Big Data

WPK1.3-D3 Good practices and recommendations on the security and resilience of Smart Home Environments

Outputs

Coherent and meaningful data on the emerging threat landscape and trends is collected

The risks in two emerging technology or application areas are assessed

MS' policies, regulations and strategies, and gaps in these are identified

ENISA's methodology for the identification of critical communication networks, links and components is developed

Policy, technical and regulatory barriers to using cloud computing in the finance sector are identified

Information on security and resilience of major eHealth infrastructures and services is collected and assessed

For all three areas the current situation in terms of cyber security and resilience is identified and assessed

Outcomes

Policy makers and public or private sector organisations receive information about NIS threats in the EU

Stakeholders of CIIs receive advice and assistance

Good practices on emerging smart infrastructures and services are developed and deployed

Results

More effective risk mitigation strategies are put in place

Relevant methods towards emerging technologies are adopted

A common approach towards security threats is developed

Opportunities of new technologies and approaches are enabled

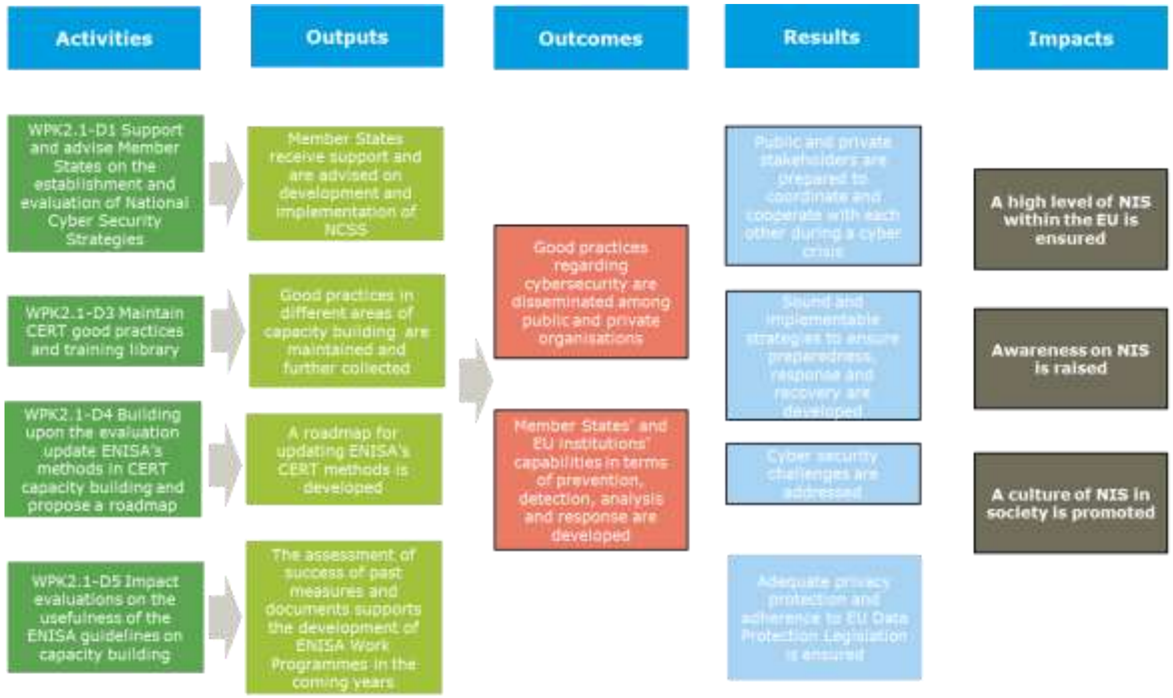
Impacts

A high level of NIS within the EU is ensured

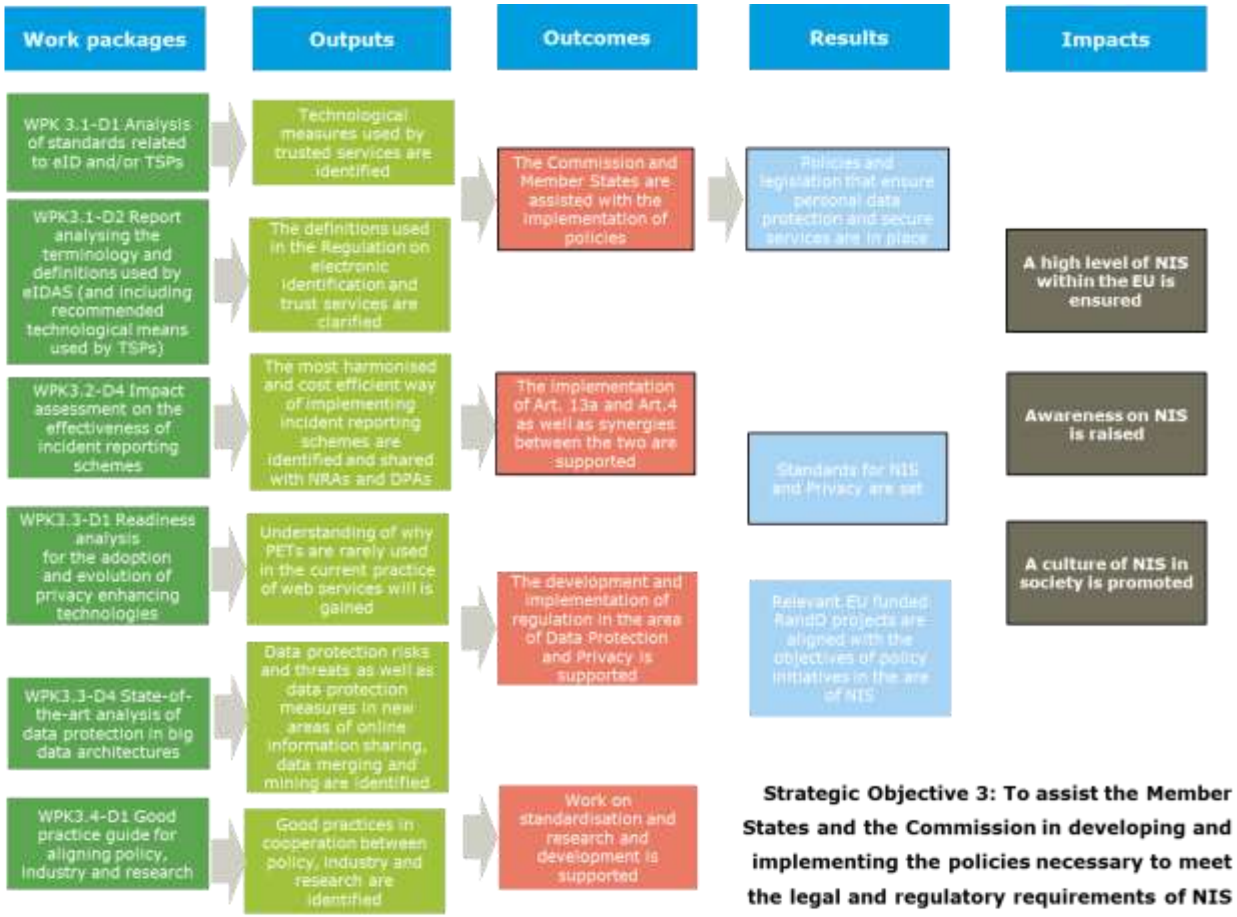
Awareness on NIS is raised

A culture of NIS in society is promoted

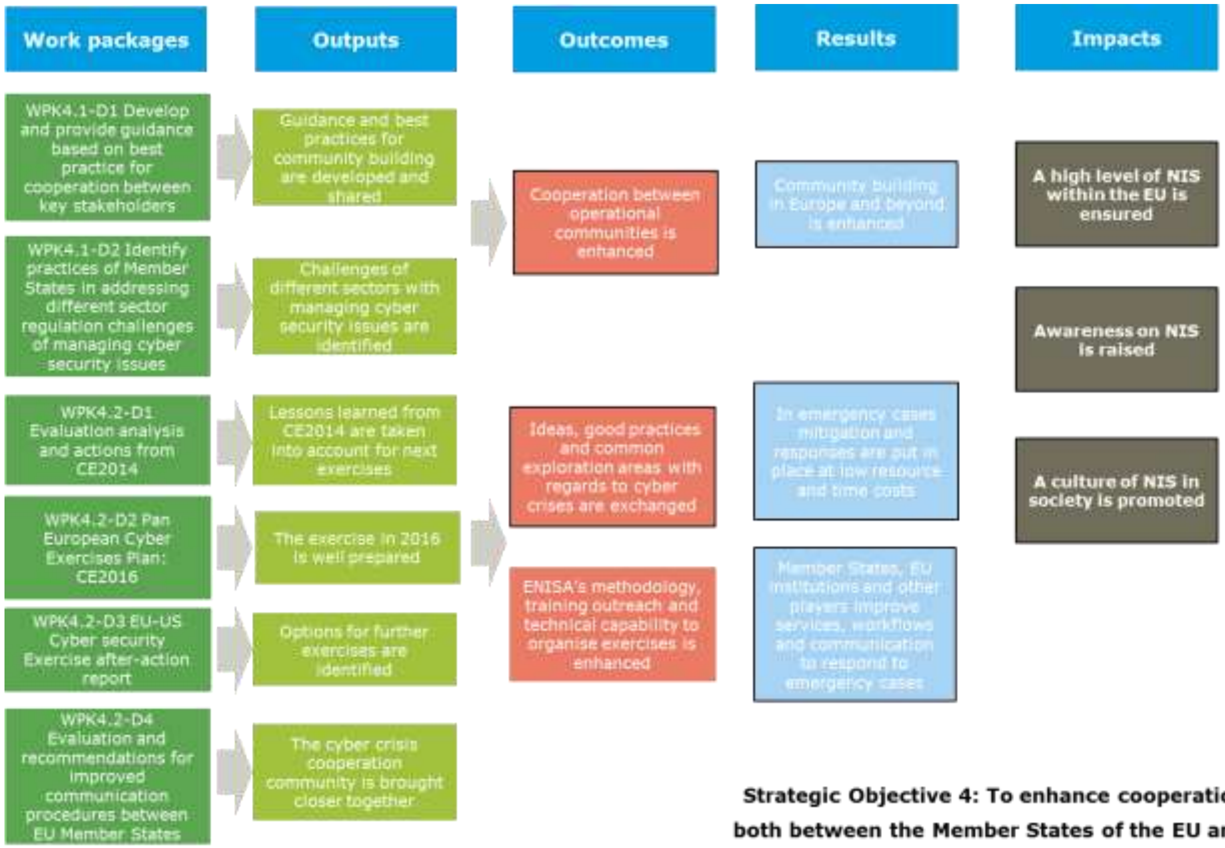
Strategic Objective 1: To develop and maintain a high level of expertise on EU actors taking into account evolutions in NIS


Activities
Outputs
Outcomes
Results
Impacts
WPK2.1-D1 Support and advise Member States on the establishment and evaluation of National Cyber Security Strategies
Member States receive support and are advised on development and implementation of NCSS
WPK2.1-D3 Maintain CERT good practices and training library
Good practices in different areas of capacity building are maintained and further collected
WPK2.1-D4 Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap
A roadmap for updating ENISA's CERT methods is developed
WPK2.1-D5 Impact evaluations on the usefulness of the ENISA guidelines on capacity building
The assessment of success of past measures and documents supports the development of ENISA Work Programmes in the coming years
Good practices regarding cybersecurity are disseminated among public and private organisations
Member States' and EU institutions' capabilities in terms of prevention, detection, analysis and response are developed
Public and private stakeholders are prepared to coordinate and cooperate with each other during a cyber crisis
Sound and implementable strategies to ensure preparedness, response and recovery are developed
Cyber security challenges are addressed
Adequate privacy protection and adherence to EU Data Protection Legislation is ensured
A high level of NIS within the EU is ensured
Awareness on NIS is raised
A culture of NIS in society is promoted

Strategic Objective 2: To assist the Member States and the Commission in enhancing capacity building throughout the EU


Work packages
Outputs
Outcomes
Results
Impacts
WPK 3.1-D1 Analysis of standards related to eID and/or TSPs
Technological measures used by trusted services are identified
WPK3.1-D2 Report analysing the terminology and definitions used by eIDAS (and including recommended technological means used by TSPs)
The definitions used in the Regulation on electronic identification and trust services are clarified
The Commission and Member States are assisted with the implementation of policies
Policies and legislation that ensure personal data protection and secure services are in place
A high level of NIS within the EU is ensured
WPK3.2-D4 Impact assessment on the effectiveness of incident reporting schemes
The most harmonised and cost efficient way of implementing incident reporting schemes are identified and shared with NRAs and DPAs
The implementation of Art. 13a and Art.4 as well as synergies between the two are supported
Awareness on NIS is raised
Standards for NIS and Privacy are set
WPK3.3-D1 Readiness analysis for the adoption and evolution of privacy enhancing technologies
Understanding of why PETs are rarely used in the current practice of web services will is gained
A culture of NIS in society is promoted
The development and implementation of regulation in the area of Data Protection and Privacy is supported
Relevant EU funded RandD projects are aligned with the objectives of policy initiatives in the are of NIS
WPK3.3-D4 State-of-the-art analysis of data protection in big data architectures
Data protection risks and threats as well as data protection measures in new areas of online information sharing, data merging and mining are identified
WPK3.4-D1 Good practice guide for aligning policy, industry and research
Good practices in cooperation between policy, industry and research are identified
Work on standardisation and research and development is supported

Strategic Objective 3: To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of NIS



Work packages
Outputs
Outcomes
Results
Impacts
WPK4.1-D1 Develop and provide guidance based on best practice for cooperation between key stakeholders
Guidance and best practices for community building are developed and shared
WPK4.1-D2 Identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues
Challenges of different sectors with managing cyber security issues are identified
WPK4.2-D1 Evaluation analysis and actions from CE2014
Lessons learned from CE2014 are taken into account for next exercises
WPK4.2-D2 Pan European Cyber Exercises Plan: CE2016
The exercise in 2016 is well prepared
WPK4.2-D3 EU-US Cyber security Exercise after-action report
Options for further exercises are identified
WPK4.2-D4 Evaluation and recommendations for improved communication procedures between EU Member States
The cyber crisis cooperation community is brought closer together
Cooperation between operational communities is enhanced
Ideas, good practices and common exploration areas with regards to cyber crises are exchanged
ENISA's methodology, training outreach and technical capability to organise exercises is enhanced
Community building in Europe and beyond is enhanced
In emergency cases mitigation and responses are put in place at low resource and time costs
Member States, EU institutions and other players improve services, workflows and communication to respond to emergency cases
A high level of NIS within the EU is ensured
Awareness on NIS is raised
A culture of NIS in society is promoted

Strategic Objective 4: To enhance cooperation both between the Member States of the EU and between related NIS communities

APPENDIX 3
M&E FRAMEWORK AND SCOREBOARD

Based on the intervention logics presented above and the work programme for 2015, we updated the original monitoring and evaluation (M&E) framework, which is intended to assess in-depth the effectiveness of the core operational activities of 2015, as a way of "zooming in" on the deliverables of the year. The M&E frameworks have been developed per strategic objective, so as to provide an overall assessment of achievements at the level of outcomes and results (please note that as evaluation criteria such as relevance, impact and coherence cuts across work streams, they have not been included here, but in the overall evaluation questions matrix presented in Appendix 1). For the outcome and result level objectives of ENISA, indicators and judgement norms are specified in the M&E framework. It also takes into account the information provided from the Key Impact Indicators (KIIs) defined for the core operational activities of 2015.

The following tables show the M&E framework per strategic objective in 2015. Outcome and result indicators which have been introduced only this year following the changes in the work programme are marked with an asterisk. A 2014 baseline to enable a comparison of performance across the years has been included (in some cases this was established in 2015 rather than 2014), as have the 2015 results. Finally, a scoreboard has been included, allowing for an assessment of the 2015 results against the listed targets.

Table 24 Strategic objective 1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)

Related WPK/SO	ENISA's objectives outcome and results level	Indicator	Baseline	2015 Figures [76]	Target	Scoreboard[77] (2015 results versus target)	Data sources
Work Packages 2015 Strategic Objective 1 To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)							
WPK 1.1	**NIS Threats Analysis**	Resources used for research and publications (staff or cost)	Baseline from 2015: EUR 245,806 2,3 FTE	EUR 245,806 2,3 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA Annual report 2015
WPK 1.2	**Improving the Protection of Critical Information Infrastructures**	Resources used for research and publications (staff or cost)	Baseline from 2015: EUR 688,253 6,6 FTE	EUR 688,253 6,6 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA Annual report 2015
WPK 1.3	**Securing emerging Technologies and Services**	Resources used for research and publications (staff or cost)	Baseline from 2015: EUR 486,603 5,3 FTE	EUR 486,603 5,3 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA Annual report 2015
WPK 1.4	**Short- and mid-term sharing of information regarding issues in NIS**	Resources used for research and publications (staff or cost)	Baseline from 2015: EUR 183,301 2,7 FTE	EUR 183,301 2,7 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA Annual report 2015
Outcome indicators							
WPK 1.1	**Policy makers and public or private sector organisations receive relevant information about NIS threats in the EU**	Policy makers and public or private sector organisations views on relevance of ENISA's deliverables about NIS threats in the EU.	87% of survey respondents confirm that the work undertaken by ENISA to identify risks and challenges has been relevant and of high quality	80% of survey respondents confirm that the work undertaken by ENISA to identify risks and challenges has been relevant and of high quality[78]	At least 70% of evaluation/survey respondents are of the opinion that the deliverables are relevant Staff/stakeholders interviewed are of the opinion that deliverables	🟩	Yearly stakeholder surveys Interviews

[76] Tracking continues in the years ahead

[77] Green = > 70%; Yellow = 51 to 69%; Red - <51%

[78] Evaluation Question 2.2

			KIIS and interviewees confirm this achievement		were relevant	🟩	
WPK 1.1		MS' views on the degree to which ENISA's deliverables complement those of other public interventions	78% of survey respondents agree that ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions	75% of survey respondents agree that ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions[79]	At least 70% of evaluation/survey respondents are of the opinion that the deliverables complement those of other public interventions Staff/stakeholders interviewed are of the opinion deliverables complement those of other public interventions and provide examples to support this	🟩	Yearly stakeholder surveys Interviews
WPK 1.2	*** Stakeholders of CIIs receive advice and assistance**	Relevant stakeholders' views on the advice and assistance received from ENISA	Baseline from 2015: 75% of survey respondents agree that ENISA's work, outputs and publications provide stakeholders of CIIs with relevant advice and assistance	75% of survey respondents agree that ENISA's work, outputs and publications provide stakeholders of CIIs with relevant advice and assistance[80]	At least 70% of evaluation/survey respondents who are stakeholders of CIIs are of the opinion to receive useful and relevant advice and assistance from ENISA CIIs stakeholders interviewed report that advice and assistance has been provided by ENISA	🟩	Yearly stakeholder surveys Interviews Case studies
WPK 1.3	* **Good practices on emerging smart infrastructures**	Public and private stakeholders agree that good practices have been disseminated by ENISA	Baseline from 2015: 88% of survey respondents agree that good	88% of survey respondents agree that good practices in NIS have been disseminated	At least 70% of evaluation/survey respondents are of the opinion that good	🟩	Yearly stakeholder surveys Interviews

[79] Survey Question 2.3

[80] Survey Question 7.15

	and services are developed and deployed		practices in NIS have been disseminated by ENISA[81]	by ENISA[82]	practices have been disseminated Staff/stakeholders interviewed are of the opinion that good practices are disseminated	🟩	Case studies
Result indicators							
SO1		Achievement of relevant KIIs	KIIs achieved	Achievement of 4/11 KIIs; partial achievement of lack of clarity in achievement of 5/11; 2 KIIs too early to judge.	Targets achieved	🟨	Annual report 2015
SO1	**More effective risk mitigation strategies are put in place**	Stakeholders' views on the degree to which use is being made of ENISA's outputs to put in place more effective risk mitigation strategies	67% of survey respondents agree that ENISA's outputs and deliverables contribute to putting in place more effective risk mitigation strategies	68% of survey respondents agree that ENISA's outputs and deliverables contribute to putting in place more effective risk mitigation strategies [83]	At least 70% of evaluation/survey respondents are of the opinion that use is being made of ENISA's outputs Staff/stakeholders interviewed are of the opinion that use is being made of ENISA's outputs listed above	🟩	Yearly stakeholder surveys Interviews
SO1	*** Relevant methods towards emerging technologies are adopted**	Stakeholders' views on the relevance of methods promoted by ENISA	Baseline from 2015: 56% of survey respondents agree that ENISA promotes relevant methods towards the adoption of emerging technologies	56% of survey respondents agree that ENISA promotes relevant methods towards the adoption of emerging technologies [84]	At least 70% of evaluation/survey respondents agree that the methods towards emerging technologies promoted by ENISA are relevant Staff/stakeholders interviewed agree that promoted methods are relevant	🟨	Yearly stakeholder surveys Interviews
SO1	*** A common**	Stakeholders' views on	Baseline from	Stakeholders	At least 70% of	🟨	Yearly stakeholder

[81] Survey Question 3.2

[82] Survey Question 3.2

[83] Evaluation Question 2.7

[84] Evaluation Question 2.10

	approach towards security threats is developed	the degree to which ENISA's activities lead to a common approach towards security threats	2015: Stakeholders interviewed (including for case study WPK 1.2) did not assess that ENISA´s activities lead to a common approach towards security threats, but assessed that ENISA´s activities supports the development of stakeholders´ expertise.	interviewed (including for case study WPK 1.2) did not assess that ENISA´s activities lead to a common approach towards security threats, but assessed that ENISA´s activities supports the development of stakeholders´ expertise.	evaluation/survey respondents agree that ENISA's activities lead to a common approach towards security threats Staff/stakeholders interviewed agree that ENISA's activities lead to a common approach towards security threats		surveys Interviews Case studies
SO1	*** Opportunities of new technologies and approaches are enabled**	Stakeholders' views on the degree to which ENISA's activities enable opportunities for new technologies and approaches	Baseline from 2015: 51% of survey respondents confirm that ENISA's activities enable opportunities for new technologies and approaches	51% of survey respondents confirm that ENISA's activities enable opportunities for new technologies and approaches[85]	At least 70% of evaluation/survey respondents agree that ENISA's activities enable opportunities for new technologies Staff/stakeholders interviewed agree that ENISA's activities enable opportunities for new technologies		Yearly stakeholder surveys Interviews

[85] Evaluation Question 2.11

Table 25 Strategic Objective 2: To assist Member States and the Commission in enhancing capacity building throughout the EU

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures[86]	Target	Scoreboard[87]	Data sources
Work Packages 2015 Strategic Objective 2: To assist Member States and the Commission in enhancing capacity building throughout the EU							
WPK 2.1	**Assist in public sector capacity building**	Resources used for research and publications (staff or cost)	EUR 168,764.26	EUR 788, 253 6,6 FTE	N/A tracking/comparison against year 1.	–	Financial data from ENISA Annual reports 2014 and 2015
WPK 2.2	**Assist in private sector capacity building**	Resources used for research and publications (staff or cost)	EUR 209,857.08	EUR 185,971 2,4 FTE	N/A tracking/comparison against year 1.	–	Financial data from ENISA Annual reports 2014 2015 ENISA evaluation form
WPK 2.3	**Assist in improving awareness of the general public**	Resources used for research and publications (staff or cost)	EUR 13,346.97	EUR 167,476 2,0 FTE	N/A tracking/comparison against year 1.	–	Financial data from ENISA Annual reports 2014 and 2015 ENISA evaluation form
Outcome indicators							
WPK 2.1	**Good practices regarding cybersecurity are disseminated among public and private organisations**	Public and private stakeholders agree that good practices have been disseminated by ENISA	Baseline from 2015: 88% of survey respondents agree that good practices in NIS have been disseminated by ENISA[88]	88% of survey respondents agree that good practices in NIS have been disseminated by ENISA[89]	At least 70% of evaluation/survey respondents are of the opinion good practices have been disseminated Staff/stakeholders interviewed are of the	🟩	Yearly stakeholder surveys Interviews

[86] Tracking continues in the years ahead

[87] Green = > 70%; Yellow = 51 to 69%; Red - <51%

[88] Survey Question 3.2

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures[86]	Target	Scoreboard[87]	Data sources
					opinion that good practices are disseminated	🟩	
WPK 2.1	**Member States' and EU institutions' capabilities in terms of prevention, detection, analysis and response are developed**	Stakeholders views on ENISA's support to developing capacities in prevention, detection, analysis and response	81% of survey respondents agree that ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States CERT trainings reported to be successful	72% of survey respondents agree that ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States [90]	At least 70% of evaluation/survey respondents are of the opinion that capacities have been developed thanks to ENISA's support Staff/stakeholders interviewed are of the opinion that capacities have been developed thanks to ENISA's support	🟩	Yearly stakeholder surveys Interviews
Result indicators							
SO2	**N/A**	Achievement of relevant KIIs	Eight KIIs achieved, one limited achievements	Achievement of 1/3 indicators; partial achievement of 1/3 indicators (target of 2017); lack of clarity in achievement where follow-up on action taken needed for 1/3 indicators (target of 2017)	Targets achieved	🟨	Annual report 2015
SO2	**Public and private stakeholders are prepared to coordinate and cooperate with**	Stakeholders' views on the degree to which they are prepared to coordinate and cooperate during a cyber crisis	71% of survey respondents agree that ENISA's support has enabled relevant stakeholders to be	68% of survey respondents agree that ENISA's support has enabled relevant stakeholders to be prepared to coordinate	At least 70% of evaluation/survey respondents are of the opinion that they are prepared	🟨	Yearly stakeholder surveys Interviews

[89] Survey Question 3.2

[90] Survey Question 3.3.

Note: The baseline specifically focuses on capacities in Member States. For this reason, the 2015 figures have also focused on capacity development at the Member State level. The alternative would have been to use Survey Question 7.16, which is similar but with a focus on the EU level. This would have included both EU and Member State level of capacity development.

Related WPK/SO	ENISA’s objectives at outcome and result levels	Indicator	Baseline	2015 Figures[86]	Target	Scoreboard[87]	Data sources
	each other during a cyber crisis		prepared to coordinate and cooperate during a cyber-crisis	and cooperate during a cyber-crisis[91]	Staff/stakeholders interviewed are of the opinion that preparedness is good	🟨	
SO2	**Sound and implementable strategies to ensure preparedness, response and recovery are developed**	Stakeholders’ views on the degree to which sound and implementable strategies to ensure preparedness, response and recovery have been developed	69% of survey respondents agree that sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA	70% of survey respondents agree that sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA[92]	At least 70% of evaluation/survey respondents are of the opinion that strategies have been developed Staff/stakeholders interviewed are of the opinion that strategies have been developed	🟩	Yearly stakeholder surveys Interviews
SO2	**Cyber security challenges are addressed**	Stakeholders’ views on the degree to which cyber security challenges are addressed	27% of survey respondents agree that cyber security challenges are adequately addressed by the Member States 29% of survey respondents agree that cyber security challenges are adequately addressed in the EU	41% of survey respondents agree that cyber security challenges are adequately addresses by the Member States [93] 45% of survey respondents agree that cyber security challenges are adequately addressed in the EU[94]	At least 70% of evaluation/survey respondents are of the opinion that cyber security challenges are addressed Staff/stakeholders interviewed are of the opinion that cyber security challenges are addressed	🟥	Yearly stakeholder surveys Interviews
SO2	*** Adequate privacy protection and adherence to EU Data Protection Legislation is ensured**	Stakeholder’s views on the degree to which ENISA’s activities foster privacy protection	Baseline from 2015: Stakeholders interviewed (including for case study WPK 2.1) agreed that ENISA´s activities	Stakeholders interviewed (including for case study WPK 2.1) agreed that ENISA´s activities foster privacy protection.	At least 70% of evaluation/survey respondents are of the opinion that ENISA’s activities foster privacy protection	🟩	Yearly stakeholder surveys Interviews Case studies

[91] Survey Question 3.6

[92] Survey Question 3.7

[93] Survey Question 3.9

[94] Survey Question 3.8

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures[86]	Target	Scoreboard[87]	Data sources
			foster privacy protection.		Staff/stakeholders interviewed are of the opinion that ENISA's activities foster privacy protection	🟩	
		Stakeholders' views on the degree to which ENISA's activities ensure adherence to EU Data Protection Legislation	59% of survey respondents agree that ENISA's activities ensure adherence to EU Data Protection Legislation.	59% of survey respondents agree that ENISA's activities ensure adherence to EU Data Protection Legislation. [95]	At least 70% of evaluation/survey respondents are of the opinion that ENISA's activities ensure adherence to EU Data Protection Legislation Staff/stakeholders interviewed are of the opinion that ENISA's activities ensure adherence to EU Data Protection Legislation	🟨	Yearly stakeholder surveys Interviews

Table 26 Strategic Objective 3: To assist the Member States and the Commission in developing and implementing the policies

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[96]	Data sources
	Work Packages 2015 Strategic Objective 3: To assist the Member States and the Commission in developing and implementing the policies						
WPK 3.1	**Provide information and advice to support policy development**	Resources used for research and publications (staff or cost)	EUR 136,217.19	EUR 233,301 2.7 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA Annual report 2015
WPK 3.2	**Assist EU MS and Commission in the**	Resources used for research and publications (staff or cost)	Baseline for 3.2 and 3.3 EUR 95,689.88	EUR 506,603 5,3 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA

[95] Survey Question 3.10

[96] Green = > 70%; Yellow = 51 to 69%; Red - <51%

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[96]	Data sources
	implementation of EU NIS regulations						Annual report 2015
WPK 3.3	**Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation**	Resources used for research and publications (staff or cost)	Baseline for 3.2 and 3.3 EUR 95,689.88	EUR 404,952 4,0 FTE	N/A tracking/comparison against year 1.	–	Financial data from ENISA Annual report 2015
WPK 3.4	**R & D, Innovation and Standardisation**	Resources used for research and publications (staff or cost)	EUR 55,044.10	248,301 2,7 FTE	N/A tracking/comparison against year 1.	–	Financial data from ENISA Annual report 2015
Outcome indicators							
WPK 3.1	**The Commission and Member States are assisted with the implementation of policies**	Policy makers views on the usefulness of the input from ENISA to implement new policies	75% of survey respondents agree that the input provided by ENISA to develop new policies for NIS in the EU is useful 61% of survey respondents agree that the input provided by ENISA to implement new policies for NIS in the EU is useful KIIs reached	75% of survey respondents agree that the input provided by ENISA to develop new policies for NIS in the EU is useful [97] 73% of survey respondents agree that the input provided by ENISA to implement new policies for NIS in the EU is useful [98]	At least 70% of evaluation/survey respondents are of the opinion that the inputs are useful and relevant Staff/stakeholders interviewed are of the opinion that inputs are useful and relevant	🟩	Yearly stakeholder surveys Interviews Annual report 2015
WPK 3.2	**The implementation of Art. 13a and Art.4 as well as**	KIIS on the support of Art 13.a and Art. 4.	KIIs reached ENISA staff reported in	KIIs achieved	Targets achieved	🟩	Annual report 2015

[97] Survey Question 2.4

[98] Survey Question 2.5

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[96]	Data sources
	synergies between the two are supported		interviews that by reporting on incidents and disseminating good examples of mitigation an aggregated view is provided and lessons and knowledge is shared			🟩	
WPK 3.3	*** The development and implementation of regulation in the area of Data Protection and Privacy is supported**	Stakeholders' views on the degree to which ENISA supports the development and implementation of Data Protection and Privacy regulation.	Baseline from 2015: 71% of survey respondents agree that ENISA's activities support the development and implementation of Data Protection and Privacy Regulation [99]	71% of survey respondents agree that ENISA's activities support the development and implementation of Data Protection and Privacy Regulation [100]	At least 70% of evaluation/survey respondents are of the opinion that ENISA supports the development and implementation of Data Protection and Privacy regulation Staff/stakeholders interviewed are of the opinion that ENISA supports the development and implementation of Data Protection and Privacy regulation	🟩	Yearly stakeholder surveys Interviews Case study
WPK 3.4	*** Work on standardisation and research and development is**	Stakeholders agree that ENISA supports standardisation and RandD	65% of survey respondents agree that the information provided by ENISA to stakeholders on	70% of survey respondents agree that the information provided by ENISA to stakeholders on	At least 70% of evaluation/survey respondents are of the opinion that ENISA supports standardisation	🟩	Yearly stakeholder surveys Interviews

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[96]	Data sources
	supported		standardization, innovation and research is relevant	standardization, innovation and research is relevant[101]	and RandD Staff/stakeholders interviewed are of the opinion that ENISA supports standardisation and RandD	🟩	
Result indicators							
SO3	**N/A**	Achievement of relevant KIIs	KIIs achieved	9/10 KIIS achieved; lack of clarity in achievement where follow-up on action taken needed for 1/2 indicators	Targets achieved	🟩	Annual report 2015
SO3	**Policies and legislation that ensure personal data protection and secure services are in place**	Stakeholders views on ENISA's outputs contribution to ensure personal data protection and secure services	50% of survey respondents agree that ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services	68% of survey respondents agree that ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services [102]	At least 70% of evaluation/survey respondents are of the opinion that ENISA's outputs contributes to the objective Staff/stakeholders interviewed are of the opinion that ENISA's outputs contributes to the objective	🟨	Yearly stakeholder surveys Interviews
SO3	**Standards for NIS and Privacy are set**	Stakeholders views on ENISA's outputs contribution to setting standards for NIS and privacy	65% of survey respondent agree that ENISA's outputs and deliverables contribute to setting standards for NIS and privacy	69% of survey respondent agree that ENISA's outputs and deliverables contribute to setting standards for NIS and privacy[103]	At least 70% of evaluation/survey respondents are of the opinion that ENISA's outputs contributes to the objective Staff/stakeholders interviewed are of the opinion that ENISA's	🟨	Yearly stakeholder surveys Interviews

[101] Survey Question 2.6

[102] Survey Question 2.8

[104] Survey Question 4.11

Deleted: ¶

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[96]	Data sources
					outputs contributes to the objective	🟨	
SO3	*** Relevant EU funded RandD projects are aligned with the objectives of policy initiatives in the area of NIS**	Stakeholder's views on the influence of ENISA's activities on coherence between EU funded RandD projects and the objectives of NIS policy	Baseline from 2015: 47% of survey respondents agree that ENISA increases coherence between EU funded R&D project and the objectives of NIS policy	47% of survey respondents agree that ENISA increases coherence between EU funded R&D project and the objectives of NIS policy [104]	At least 70% of evaluation/survey respondents are of the opinion that ENISA's activities foster coherence Staff/stakeholders interviewed are of the opinion that ENISA's activities foster coherence	🟥	Yearly stakeholder surveys Interviews

Table 27 Strategic Objective 4: To enhance cooperation both between the Member States of the EU and between related NIS

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[105]	Data sources
Work Packages 2015 Strategic Objective 4: To enhance cooperation both between the Member States of the EU and between related NIS							
WPK 4.1	**Support for EU cooperation initiatives amongst NIS – related communities in the context of the EU CSS**	Resources used for research and publications (staff or cost)	EUR 100,955.00	EUR 329,777 4,6 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA Annual report 2015
WPK 4.2	**European cyber crisis cooperation through exercises**	Resources used for research and publications (staff or cost)	EUR 158,081.79	617,428 6,0 FTE	N/A – tracking/comparison against year 1.		Financial data from ENISA Annual report 2015

[104] Survey Question 4.11

[105] Green = > 70%; Yellow = 51 to 69%; Red - <51%

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[105]	Data sources
		Outcome indicators					
WPK 4.1	**Cooperation between operational communities is enhanced**	Stakeholders views on enhanced cooperation in operational communities	70% of survey respondents agree that ENISA ‘s support has contributed to enhanced cooperation in operational communities Interviewees reported that there was a need to strengthen and develop relationships with senior level and decision makers at national level Case study results suggest that CE2014 enhanced cooperation between operational communities to a limited extent	82% of survey respondents agree that ENISA ‘s support has contributed to enhanced cooperation in operational communities[106]	At least 70% of evaluation/survey respondents are of the opinion that cooperation has been enhanced Staff/stakeholders interviewed are of the opinion that cooperation has been enhanced	🟩	Yearly stakeholder surveys Interviews
WPK 4.2	**Ideas, good practices and common exploration areas with regards to cyber crises are exchanged**	Stakeholders views on sharing of information, ideas and common areas of interest	76% of survey respondents agree that ENISA effectively supports the sharing of information, ideas and common areas of interest among	90% of survey respondents agree that ENISA effectively supports the sharing of information, ideas and common areas of interest among stakeholders[107]	At least 70% of evaluation/survey respondents are of the opinion that cooperation has contributed to sharing of ideas with regards to cyber crisis	🟩	Yearly stakeholder surveys Interviews

[106] Survey Question 4.5

[107] Survey Question 4.2

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[105]	Data sources
			stakeholders		Staff/stakeholders interviewed are of the opinion that cooperation has contributed to sharing of ideas with regards to cyber crisis	🟩	
		MS' views on the degree to which ENISA's outputs complement those of other public interventions	84% of survey respondents (excluding industry stakeholders) agree that ENISA's support to cooperation between stakeholders complements other public interventions	83% of survey respondents (excluding industry stakeholders) agree that ENISA's support to cooperation between stakeholders complements other public interventions[108]	At least 70% of evaluation/survey respondents are of the opinion that the outputs complement those of other public interventions Staff/stakeholders interviewed are of the opinion that outputs complement those of other public interventions and provide examples to support this	🟩	Yearly stakeholder surveys Interviews
WPK 4.2	*** ENISA's methodology, training outreach and technical capability to organise exercises is enhanced**	Types of training participants	Baseline 2015: In total 29 EU and EFTA countries are participating in the planning process of Cyber Europe 2016. Evidence on the training participants during 2015 was not available at the time of the evaluation		ENISA reaches new stakeholders with trainings Staff/stakeholders interviewed are of the opinion that outputs complement those of other public interventions and provide examples to support this		Training participant lists Interviews
		Training participants' and	81% of survey	81% of survey	Evaluations of trainings	🟩	Evaluations of

[108] Survey Question 4.3

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[105]	Data sources
		ENISA trainers' perception of methodology and technical capabilities	respondents agree that ENISA effectively shares lessons learned from cyber security exercises with other communities and sectors	respondents agree that ENISA effectively shares lessons learned from cyber security exercises with other communities and sectors[109]	show a positive result At least 70% of evaluation/survey respondents are of the opinion that ENISA's training methodology and technical capabilities have improved	🟩	trainings Yearly stakeholder surveys
Result indicators							
SO4	**N/A**	Achievement of relevant KIIs	KIIs achieved	3/4 KIIs achieved; partial achievement of ¼ (target of 2016)	Targets achieved	🟩	Annual report 2015
SO4	**Community building in Europe and beyond is enhanced**	Stakeholders' views on the degree to which community building in Europe and beyond is enhanced	78% of survey respondents agree that the support form ENISA has contributed to enhancing community building in Europe and beyond	85% of survey respondents agree that the support form ENISA has contributed to enhancing community building in Europe and beyond[110]	At least 70% of evaluation/survey respondents are of the opinion that community building in Europe and beyond is enhanced Staff/stakeholders interviewed are of the opinion that community building in Europe and beyond is enhanced	🟩	Yearly stakeholder surveys Interviews
SO4	**In emergency cases, mitigation and responses are put in place at low resource and time costs**	Stakeholders' views on the degree to which mitigation and responses are put in place at low resource and time costs Evidence of mitigation and responses from real incidents	49% of survey respondents agree that ENISA's support enabled putting in place emergency mitigation and responses at low resources and time	54% of survey respondents agree that ENISA's support enabled putting in place emergency mitigation and responses at low resources and time cost[111]	At least 70% of evaluation/survey respondents are of the opinion that mitigation and responses are put in place at low resource and time costs Staff/stakeholders	🟨	Yearly stakeholder surveys Interviews Incident reports

[109] Survey Question 4.4

[110] Survey Question 4.9

[111] Survey Question 4.8

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[105]	Data sources
			cost Case study findings suggest that cyber security exercises support that in emergency cases, mitigation and responses are put in place (at low resources and time costs), by providing a good opportunity to test and improve cyber security capabilities and take action at national level in relation to any lessons learned		interviewed are of the opinion that mitigation and responses are put in place at low resource and time costs Clear evidence of efficient mitigation and responses from real incidents is provided		
SO4	**Member States, EU institutions and other players improve services, workflows and communication to respond to emergency cases**	Stakeholders' views on the degree to which services, workflow and communication to respond to crisis has been improved	68% of survey respondents agree that ENISA's support has improved services, workflow and communication among stakeholders to respond to crises Case study findings suggest that CE 2014 lead to improvements in MS' workflows and communication to respond to emergency cases at	68% of survey respondents agree that ENISA's support has improved services, workflow and communication among stakeholders to respond to crises [112]	At least 70% of evaluation/survey respondents are of the opinion that services, workflow and communication to respond to crisis has been improved Staff/stakeholders interviewed are of the opinion that services, workflow and communication to respond to crisis has been improved		Yearly stakeholder surveys Interviews

[112] Survey Question 4.6

Related WPK/SO	ENISA's objectives at outcome and result levels	Indicator	Baseline	2015 Figures	Target	Scoreboard[105]	Data sources
			national level				
		Technical capacity has increased among involved stakeholders	42% of survey respondents agree that technical capacity had increased among involved stakeholders Case study interviews confirm increase in technical capacity of participants	52% of survey respondents agree that technical capacity had increased among involved stakeholders [113]	At least 70% of evaluation/survey respondents are of the opinion that technical capacity has been improved to respond to crisis has been improved Staff/stakeholders interviewed are of the opinion that technical capacity to respond to crisis has been improved		Yearly stakeholder surveys Interviews
		ENISA staff report on the degree to which the follow-up actions (short, medium, long term) with a deadline of end of year n in the after action reports have been implemented	N/A		Follow up targets met		Review of follow up reports
		Achievement of relevant KIIs			Targets achieved		Annual report 2015

[113] Survey Question 4.7

APPENDIX 4
KEY ACHIEVEMENTS

The table below presents an assessment of the extent to which the deliverables under review as part of this evaluation (i.e. those with a value of above EUR 30,000) have achieved their Key Impact Indicators (KIIs), as set out in the annual work programme and annual activity report 2015 (draft). An analysis of these results is presented in section 4.2.1 of the main report.

Strategic objective 1: To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS).

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
WPK 1.1 – NIS Threats Analysis	D1	Annual Threat Analysis/Landscape Report (Q4, 2015)	• Engage 10 public and 10 private stakeholders in the Threat Analysis/Landscape process. These stakeholder should participate in the validation of the work	• **Achieved**: More than 10 public and 10 private stakeholders contributed in the Threat Analysis/Landscape process as well as the validation of the work.	"ENISA Threat Landscape 2015"
	D2	Risk Assessment on two emerging technology/application areas (Q4, 2015)	• Engage 10 public and 10 private stakeholders in the risk assessment of each emerging technologies/sector. These stakeholder should participate in the validation of the work	• **Achieved**: More than 10 public and 10 private stakeholders contributed to the risk assessment of	"Big Data Threat Landscape" "Threat Landscape and Good Practice Guide for Software Defined

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
			• 5 MS use by 2016 ENISA's Threat Analysis/Landscape process in their national risk management processes. • 10 private stakeholders use by 2016 ENISA's Threat Analysis/Landscape process in their corporate risk management processes.	each emerging technologies/sector as well as the validation of the work • **Too early to judge**: This impact can be evaluated only in 2016 [RT – this will be updated before end of review period when data will become available.] • **Too early to judge**: This impact can be evaluated only in 2016[RT – this will be updated before end of review period when data will become available.]	Networks/5G"
WPK1.2 Improving the protection of critical information infrastructures	D1	Stock Taking, Analysis and Recommendations on the protection of CIIs (Q3/2015)	• By 2017, 8 MS use ENISA's findings and good practices in their national CIIP strategies	• **Unclear whether achieved - Participation in workshop, but unclear whether use made of findings and good practices**: One workshop in September about CIIP. More than 8 MS participated in the workshop, more than 16 MS took part in interviews and surveys providing input for the study.	"Stocktaking, Analysis and Recommendations on the protection of CIIs"
	D2	Methodology for the identification of Critical Communication Networks, Links, and Components (Q4/2015)	• Engaging 8 public and 8 private stakeholders (ISP, IXPs, Telcos) in the development of the methodology on internet interconnections	• **Partially achieved - Public stakeholder target achieved but**	"Communication network interdependencies in smart grids"

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
			• 5 MS and 5 private stakeholders use ENISA's recommendations on finance in their corporate/national risk assessment and management approach	**only 5 private stakeholders:** One workshop in October about communication network dependencies for smart grids study (25 experts from national authorities and critical infrastructure operators in Europe) and one meeting in November of the Internet Infrastructure Security and Resilience Reference group of experts (INFRASEC 14 experts: 2 cyber sec agencies, 3 major IXPs in Europe, 2 Internet security research organization) - Study completed and dedicated resilience portal area about Internet threats created.	
	D4	Recommendations and Good Practices for the use of Cloud Computing in the area of Finance Sector (Q4/2015)	• 5 MS and 5 stakeholders use of ENISA's recommendations on eHealth in their corporate / national risk assessment and management approach	**Achieved**: One workshop in October in cooperation with European Banking Authority (EBA). In this event participated 26 EU national financial regulators, 12 EU private banks and 4 major Cloud service providers -The Expert Group in Finance was engaged and on average 15 experts from financial private sector participated.	"Secure Use of Cloud Computing in the Finance Sector"

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
	D5	Good Practices and Recommendations on resilience and security of eHealth Infrastructures and Services (Q4/2015)		**Achieved**: Participation in workshop of 10 MS, 10 eHealth providers and the EC - twelve MS participated in the study/survey	"Security and Resilience in eHealth Infrastructures and Services"
WPK1.3 Securing emerging Technologies and Services	D1	Good Practices and Recommendations on the Security and Resilience of Intelligent Transportation Systems (Q4/2015)	• By 2016, 5 MS and 8 private stakeholders use ENISA's recommendations on smart cities in their corporate risk assessment and management approach	**Unclear whether achieved - Participation in workshop, but unclear whether use made of recommendations**: One workshop in October about Security in Transport and Smart Cities. Co-organisation with DG MOVE. 22 participants attended the workshop from 12 MS as well as 1 non-EU country (7 participants from public sector, 15 participants from private sector). - Twelve MS participated in the study	"Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations" "Architecture model of the transport sector in Smart Cities"
	D2	Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4/2015)	• By 2016, 5 MS and 8 private stakeholders use ENISA's recommendations on big data in their corporate risk assessment and management approach	**Partially/unclear whether achieved – Participation in workshop by private sector only and unclear whether use made of recommendations:** 21 entities from private sector participated in the survey on the Big Data security. The following sectors were represented - Finance, Energy, Telecom, Research and Academia.	"Big Data Security"
	D3	Good Practices and Recommendations on the Security and Resilience of Big Data Services (Q4/2015)	• By 2016, 8 MS and 8 private stakeholders use ENISA's recommendations on Smart Home Environments in their corporate risk assessment and management approach	**Partially/unclear whether achieved – Public stakeholder target**	"Security and Resilience of Smart Home

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
				achieved but only 6 public stakeholders and unclear whether use made of recommendations: One workshop in October about Security in Transport and Smart Cities. Co-organisation with DG MOVE. 20 participants attended to the workshop from 10 MS as well as 1 non-EU country (6 participants from public sector, 14 participants from private sector). - Twelve MS participated in the study	Environments"

Strategic objective 2: To assist the Member States and the Commission in enhancing capacity building throughout the EU

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
WPK 2.1. Assist in public sector capacity building	D1	Support and Advise Member States on the establishment and evaluation of National Cyber Security Strategies (NCSS) (Q4/2015)	- By 2017, 8 MS use ENISA's recommendations and good practices on National Cyber Security Strategies.	**Partially achieved as at 2015**: Two workshops in 2015 together with the EU Presidency (Riga: 30 participants, 15 form MS; Luxembourg: 28 participants, 18 from MS), 4 MS created their national cyber security strategy based on ENISA recommendations (till November 2015), ENISA NCSS map the most popular webpage (features update). In 2016 ENISA will continue work on this topic through updating the NCSS online map, creating training material in a training platform and updating the good practice guide.	Workshop September 2015

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
	D3	Maintaining CERT good practice and training library (Q4/2015)	• More streamlined CERT exercise and training material with CERT and other operational communities' services and methodologies.	• **Achieved**: ENISA's start-up train the trainer program. 1st workshop for CSIRT trainers in Europe held in September to streamline CSIRT training material and training methodology development (24 educators from 18 MS including GEANT/TRANSITS; FIRST).	Technical training resources have been provided Handbooks published: "Mobile Threats Incident Handling. Handbook, Document for teachers" ; "Introduction to advanced artefact analysis. Handbook, Document for teachers"; "Advanced dynamic analysis. HANDBOOK, DOCUMENT FOR TEACHERS"; "Advanced static analysis. Handbook, Document for teachers"
	D4	Building upon the evaluation update ENISA's methods in CERT capacity building and propose a roadmap (Q4/2015)	• By 2017, Improved operational practices of CERTs in at least 15 MS (on-going support with best practices development)	• **Unclear whether achieved – Additional material provided and MS participation in workshop, but unclear whether operational practices improved as at 2015**: Added Good practice guide on Vulnerability disclosure to the ENISA's online library for CSIRT services and operational practice improvement. The annual CSIRT workshop for national and governmental CSIRTs held in May in Latvia to discuss and address 'the CSIRT role and services during the EU Presidency' topic (40 participants from 17 MS).	"Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations"

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
	D5	Impact evaluation on the usefulness of the ENISA guidelines on capacity building. (Q4/2015)	None indicated	None indicated	"ENISA's CSIRT-related capacity building activities"
WPK. 2.2. Assist in private sector capacity building		No deliverables above EUR 30,000			
WPK. 2.3. Assist in improving awareness of the general public		No deliverables above EUR 30,000			

Strategic objective 3: To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
WPK 3.1. Provide information and advice to support policy development	D1	Analysis of standards related to eID and/or TSPs (Report, Q4 2015)	• Engage at least 5 key sector actors in launching and establishment of a forum that brings together 3 communities, namely: trust service providers from the EU Trusted List, conformity assessment bodies and supervisory authorities. The degree of activity of the relevant key sector actors in the forum is of importance to its success. • Validations by at least 5 representatives from different MS of the contribution to the implementation of the Regulation on electronic identification and trusted	• **Achieved**: The 1st TSP Forum was organised at the end of June 2015. The forum was attended by more than 100 participants and by representatives from all key sector actors from many EU MS. • **Achieved**: The participants of the eIDAS TF were involved throughout this work also contributing at all stages of the peer review.	"Analysis of standards related to Trust Service Providers - Mapping of requirements of eIDAS to existing standards

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
			services for electronic transactions.		
	D2	Report analysing the terminology and definitions used by eIDAS and (including recommended technological means used by TSPs) (Report, Q4 2015)			"Qualified Website Authentication Certificates"
WPK 3.2. Assist EU MS and Commission in the implementation of EU NIS regulations	D4	Impact assessment on the effectiveness of incident reporting schemes (e.g. Art13a and Art 4) (Q4/2015)	• By 2017, 12 MS make direct use of the outcomes of article 13 a work by explicitly referencing it or by adopting it at nationally level • By 2017, 10 MS implement recommendations by ENISA on implementing and enforcing article 4	• **Achieved as at 2015**: A study on the impact assessment of Art. 13a in EU is published. 23 countries have responded that they have implemented the Art. 13 requirements (although the real number is greater than this), and on average 15 of them (more than 60%) declared that they have used different work produced by the group in their national implementation and work. More than this, 19 (82%) NRAs are currently satisfied with the current work model of Art. 13a expert group, drafting and agreeing on common technical guidelines and sharing experiences. • **Unclear whether achieved – MS participation in workshop, but unclear whether recommendations implemented as at 2015:** 12 MS participated in ENISA's survey on article 4 data breaches. Workshop organised by EC on data breaches of article 4 and more than 20 MS participated.	"Impact evaluation on the implementation of Article 13a incident reporting scheme within EU"
WPK 3.3 Assist EU	D1	Readiness analysis for the adoption and	▪ At least 5 representatives from	• **Achieved**: 6 EU MS	"Readiness Analysis for

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
MS and Commission in the implementation of NIS measures of EU data protection regulation		evolution of privacy enhancing technologies	different MSs contributing to ENISA guidelines and best practice recommendations regarding Privacy Enhancing Technologies ▪ At least 10 actors in the field validating the results of the studies ▪ More than 80 participants in APF’15 (researchers, policy makers and industry participants)	representatives contributed to the report also supporting in the peer review stages. • **Achieved**: 12 representatives of different sector actors contributed to the various peer review stages of the work. • **Achieved**: APF'2015 was attended by more than 100 participants. The conference gathered increased interest.	the Adoption and Evolution of Privacy Enhancing Technologies"
	D4	State-of-the-art analysis of data protection in big data architectures (Q4 2015)			"Privacy by design in big data"
WPK 3.4. R&D, Innovation and Standardisation	D1 & D2	Good Practice Guide for aligning Policy, Industry and Research (Q4/2015) Standardisation Gaps in Cyber Security (Q4/2015)	• Support at least 10 key sector actors involved in EU funded R&D programs (H2020) in the area of NIS in defining priorities. • Engage at least 5 MS representatives from at least 3 MSs in the work of the ETSI CEN CENELEC Cyber Security Coordination Group (CSCG) • Engage at least 5 MS representatives through at least 1 workshop organized in collaboration with the research (H2020) and standardization communities.	• **Achieved**: 4 meetings of the respective expert group were organised in 2015. On average, more than 10 sector actors' representatives’ participated in each one of them. • **Achieved**: 5 representatives from 3 MSs national standardisation authorities contributed to this work and the various meetings of the expert group. • **Achieved**: ENISA organised 1 workshop in October 2015 attended by over 20 participants. More than 5 MS representatives attended the workshop.	"Governance framework for European standardisation" "Definition of Cybersecurity - Gaps and overlaps in standardisation"

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities

Strategic objective 4: To enhance cooperation both between the Member States of the EU and between related NIS communities

Work packages	No of deliverable	Title of deliverable	Measuring work package impact (according to Work Programme 2015)	Achieved Results (according to Annual Activity Report 2015)	Publications and activities
WPK 4.1 Support for EU cooperation initiatives amongst NIS–related communities in the context of the EU CSS	D1	Develop and provide guidance based on best practice for cooperation between key stakeholder communities (Trust building for and reaching out to new communities) (CERTs, CIIP community, Law Enforcement, Financial Services; Data Protection, etc.) (Q4/2015)	• At least 2 new operational communities will be identified and contacted for the purpose of identifying a mutually satisfactory ways to collaborate (CERTs, LEA, EU Financial service, Data Protection, CIIP community, etc.)	• **Achieved**: Aviation and ATM communities were identified and contacted to set up a cooperation in the incident response area. In addition, LEA and CSIRT communities were involved in project to address common taxonomy for those communities in order to advance the mutual way of collaboration.	"Information sharing and common taxonomies between CSIRTs and Law Enforcement" "Update on CSIRT baseline capabilities"
	D2	Identify practices of Member States in addressing different sector regulation challenges of managing cyber security issues (Q4/2015	• By 2016, at least 15 MS are familiar with practices in addressing different sector regulation challenges of managing cyber security issues.	• **Partially achieved as at 2015 – MS participation in development of report (step 1), but degree of “familiarity” unclear**: First step - published report on “Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches”; The contribution to the report was done in cooperation with the ENISA NLO network from all 28 MS.	"Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches"

WPK 4.2. European cyber crisis cooperation through exercises	D1	Evaluation Analysis and Actions from CE2014 (restricted report, Q2 2015)	- At least 25 EU MS and EFTA countries confirm their support for pan European Cyber Exercises - At least 25 MS are familiar with and use the cross border cyber crisis EU Standard Operational Procedures by 2016	- **Achieved**: In total 29 EU and EFTA countries are participating in the planning process of Cyber Europe 2016. - **Achieved**: All countries involved in the Cyber Europe series of exercises are familiar with the cyber crisis cooperation SOPs	The restricted version shared with EU MS includes lessons learned from the 2014 pan European Exercises, including 33 actions to follow up in order to improve the cybersecurity preparedness in the EU. A public version is available online at ENISA's web site
	D2	Pan European Cyber Exercises Plan: CE2016 (restricted report, Q4 2015)			The deliverable is limited, shared with ENISA MB on November 2015.
	D3	EU-US Cybersecurity Exercise after-action Report[2] (public/restricted report, Q2 2015)			The deliverable is limited, shared with ENISA MB on November 2015.
	D4	Evaluation and recommendations for improved communication procedures between EU MSs (public/restricted report, Q4 2015)			"Common practices of EU-level crisis management and applicability to cyber crises"

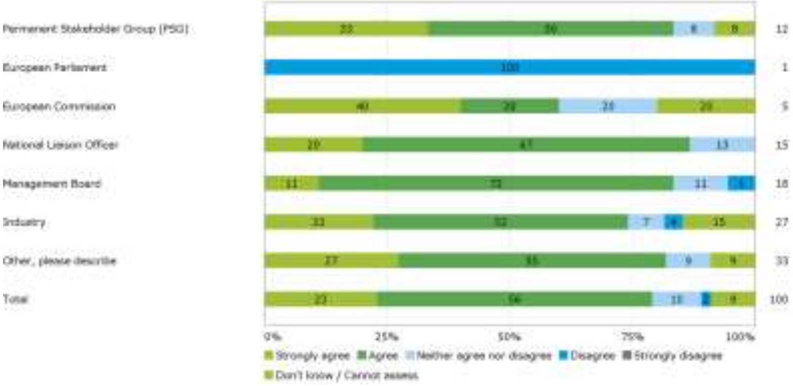
APPENDIX 5
SUMMARY OF RESPONSES TO THE SURVEY

The following presents the full survey results, an analysis of which is provided in the main body of this report.

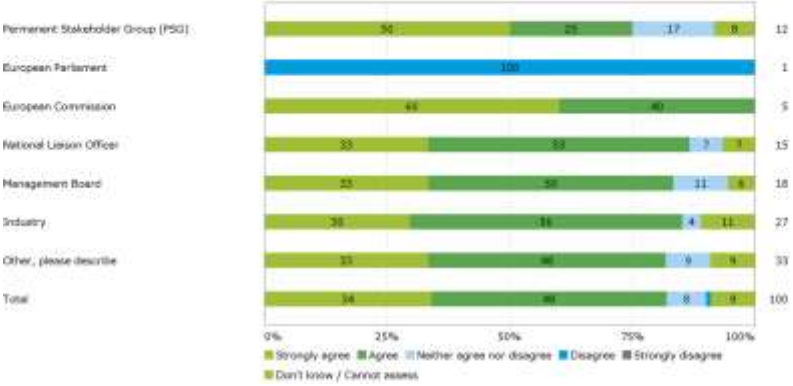
1. RELEVANCE OF ENISA’S WORK

Please rate the extent to which you agree or disagree with the following statements concerning ENISA’s support to EU Policy in National Information Security (NIS):

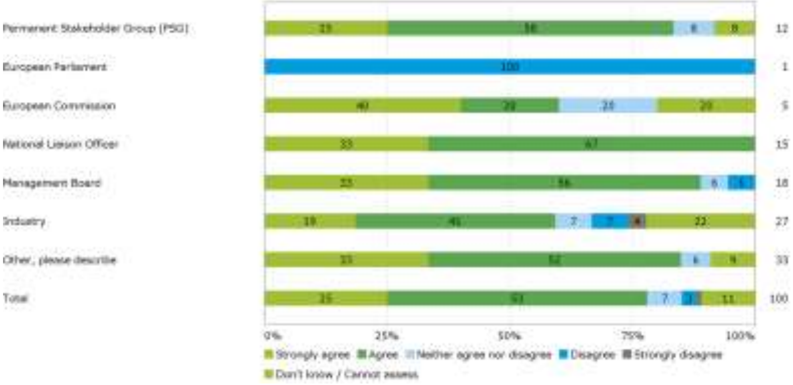
1.1 The scope and objectives of ENISA’s work are relevant to responding to the needs for NIS in the Member States



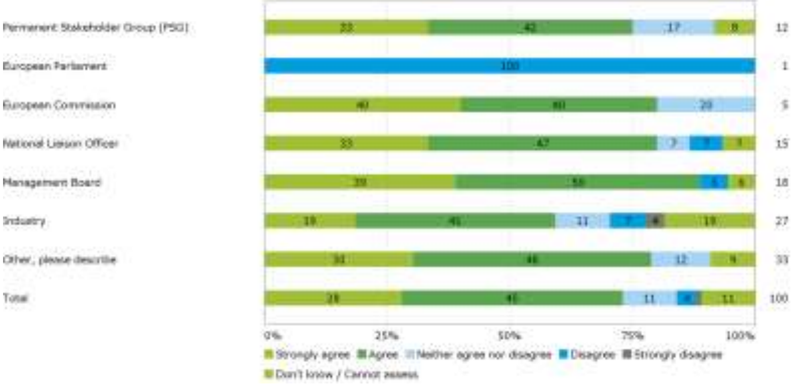
1.2 The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the EU



1.3 The outputs produced by ENISA are responding to the needs for NIS in the Member States



1.4 The outputs produced by ENISA are responding to the needs for NIS in the EU

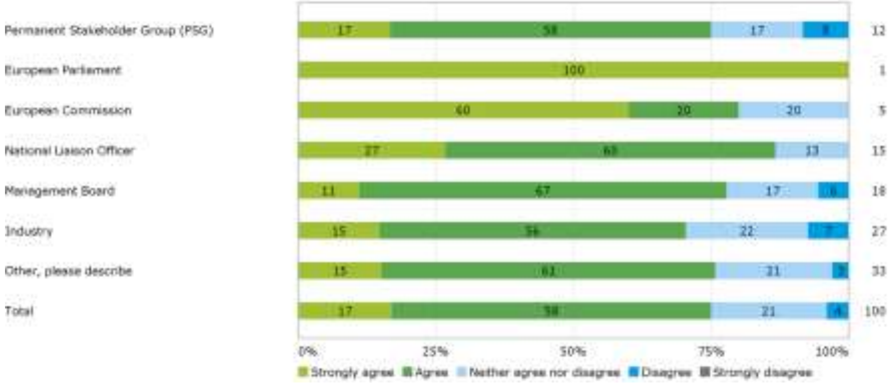


1.5 Please provide additional comments as relevant:

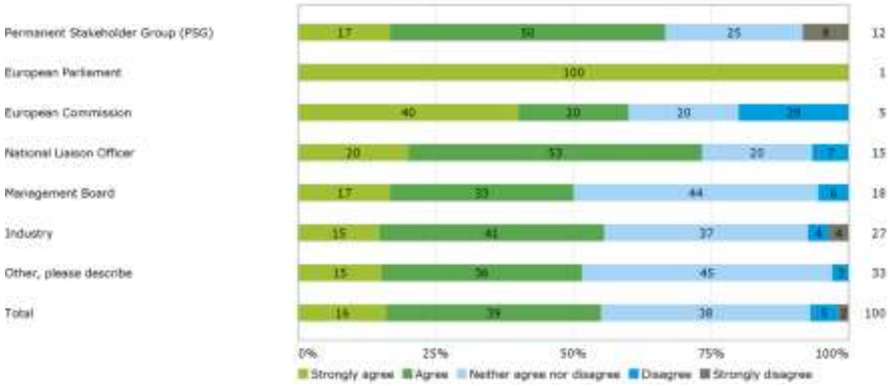
European Commission	National Liaison Officer / Management Board	Management Board / Industry	Industry / Other	Permanent Stakeholder Group (PSG) / Management Board / Other	Other
• ENISA's range of action is limited by its mandate	• ENISA mandate and resources limit impact agency should have on NIS in EU	• Most work is related to big enterprises, SME needs are rarely supported	• I think we need to look at ways to ensure the outputs are being taken on board by the relevant parties	• ENISA is the main driver	• Although I generally agree with the scope, objectives and outputs, I think they should be enlarged. • From my experience NIS is the Abbreviation for Network Information Security - not national Information security. National Information Security is hard to define because it will differ from Member State to Member State. Should NIS be interpreted more generally and include Article 13a of the telecom directive ?

Please rate the extent to which you agree or disagree with the following statements concerning ENISA's ability to meet expectations:

1.6 ENISA is effectively meeting stakeholder expectations



1.7 It is clear what ENISA expects from stakeholders

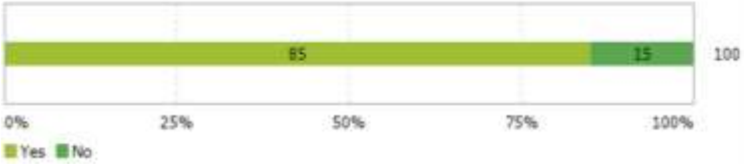


1.8 Please provide additional comments as relevant:

National Liaison Officer / Management Board	National Liaison Officer	Permanent Stakeholder Group (PSG) / Management Board / Other	Other
• ENISA meet expectations that are expressed and are not out of the agency remit • In the foels of cyber exercises there is sometimes a different set of expectations between some of the member states and ENISA	• ENISA is doing well to collect inputs and feedback on WPs and those who participate are I think generally satisfied with the outcome.	• ENISA's view and goal is clear, but not necessary easy to achieve	• From a distant view, it seems that ENISA is centralized to particular issues and maybe a part of the stakeholders is left out. E.g. Energy operators / Retail Markets/ Big industrial consumers… I am not sure if ENISA’s expectations from Stakeholders are communicated thoroughly, especially in national level.

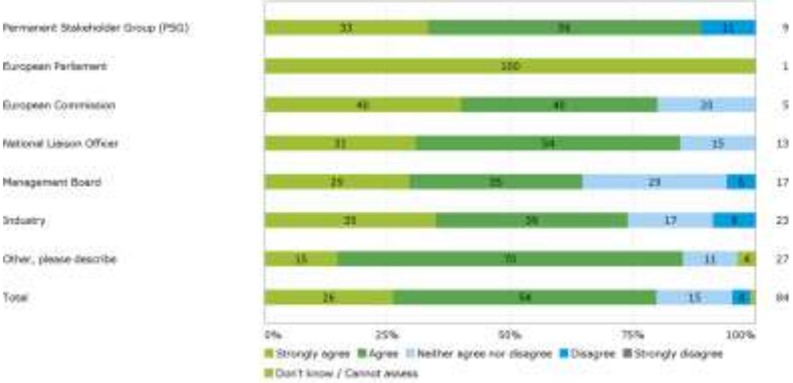
2. EFFECTIVENESS: SUPPORT TO EU POLICY BUILDING

2.1 Are you familiar with ENISA’s work on developing and maintaining a high level of expertise related to NIS, facilitating voluntary information exchange, establishing mutual interactions, and/or contributing to EU policy initiatives and supporting the EU in education, research and standardisation?

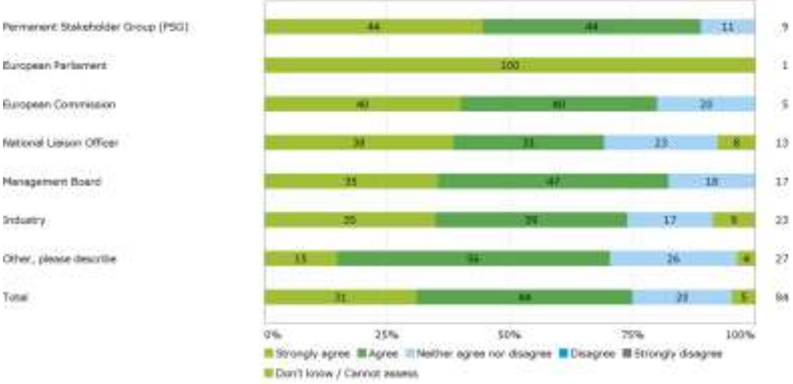


Please rate the extent to which you agree or disagree with the following statements concerning ENISA’s support to EU Policy in NIS:

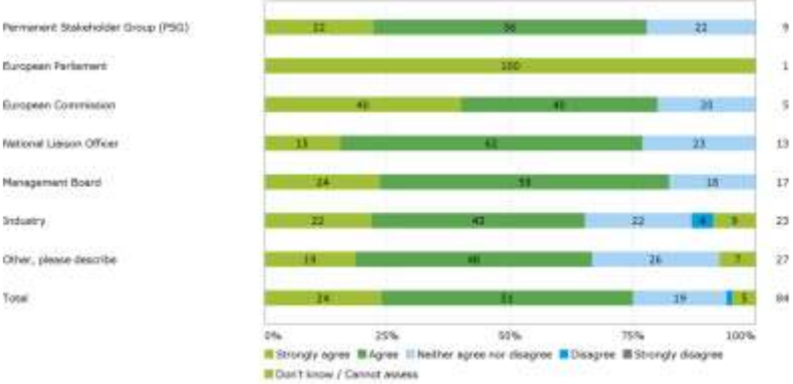
2.2 ENISA’s deliverables about NIS threats in the EU are relevant and of high quality



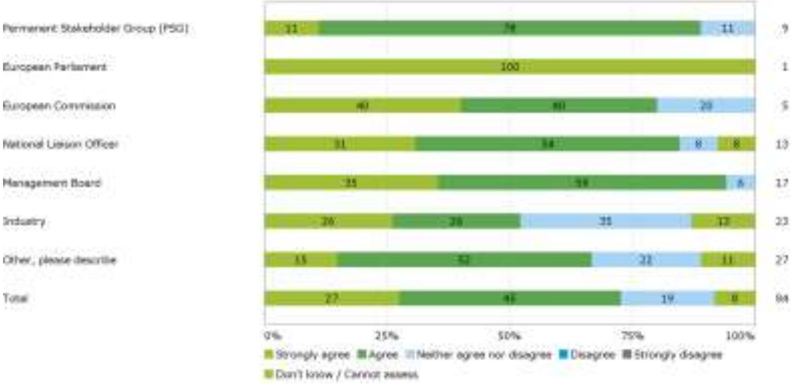
2.3 ENISA’s deliverables to support NIS policy at the EU level complement those of other public interventions



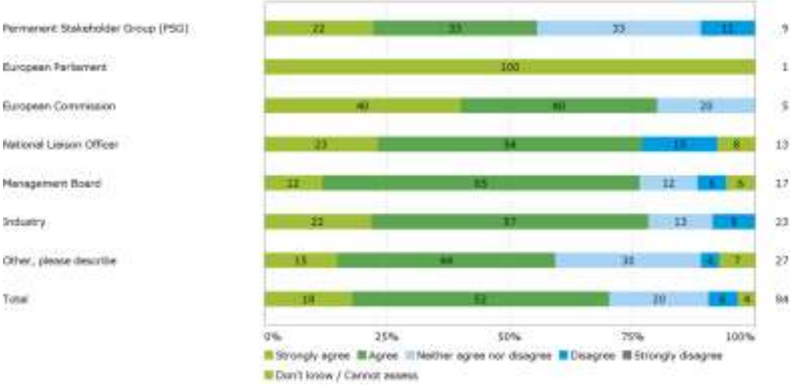
2.4 The input provided by ENISA to develop new policies for NIS in the EU is useful



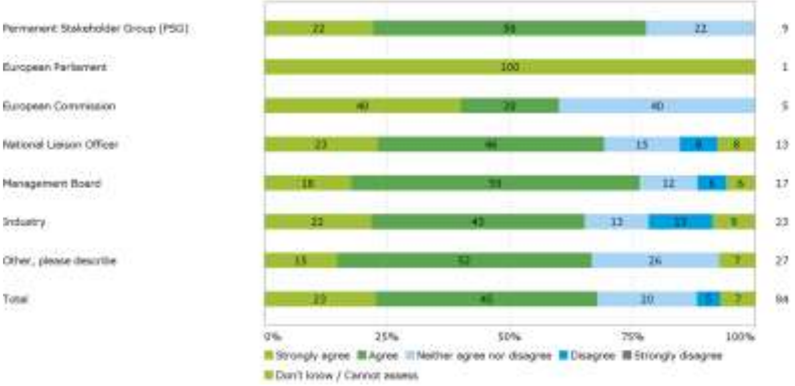
2.5 The input provided by ENISA to implement new policies for NIS in the EU is useful



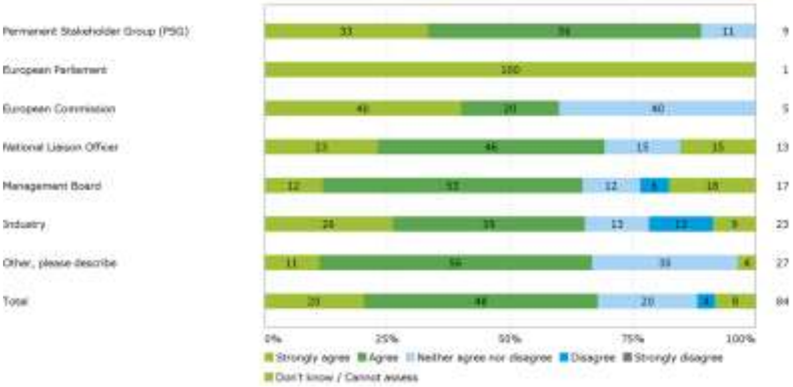
2.6 ENISA provides stakeholders with relevant information on standardisation, innovation and research



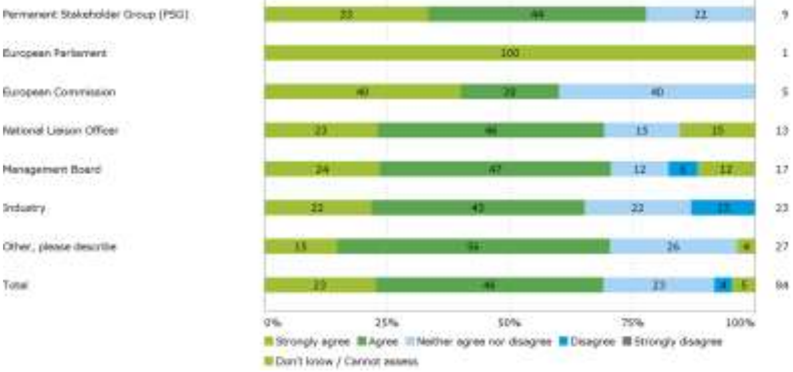
2.7 ENISA's outputs and deliverables contribute to putting in place more effective risk mitigation strategies



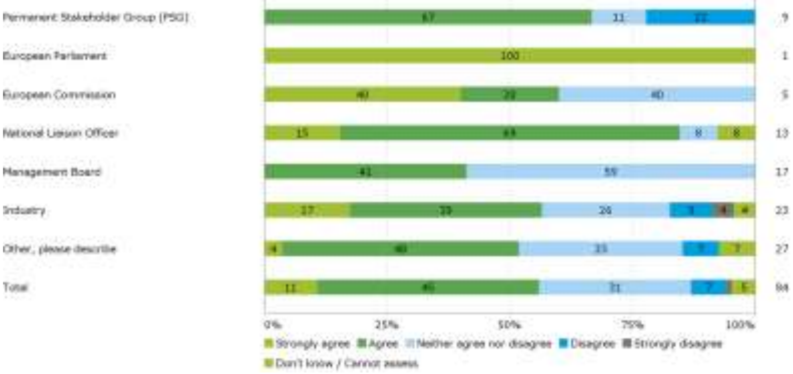
2.8 ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services



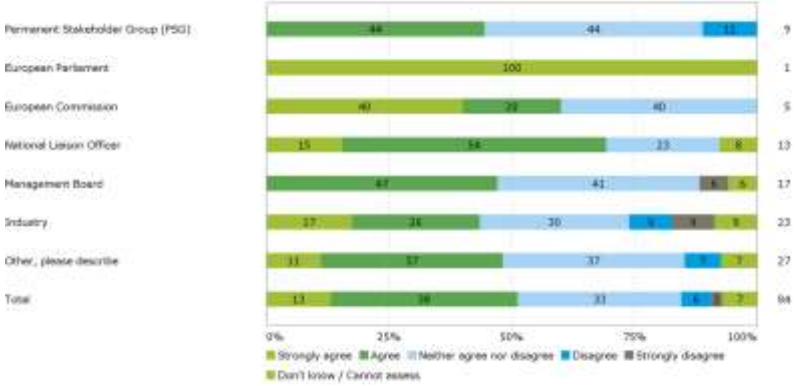
2.9 ENISA’s outputs and deliverables contribute to setting standards for NIS and privacy



2.10 ENISA promotes relevant methods towards emerging technologies



2.11 ENISA's activities enable opportunities for new technologies and approaches

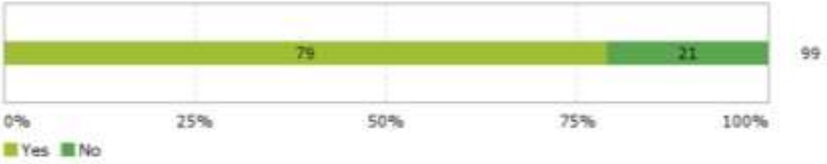


2.12 Please provide additional comments as relevant:

National Liaison Officer / Management Board	Permanent Stakeholder Group (PSG) / Management Board / Other	Other
The external effects of the several expert document seems rather low	**ENISA has in certain areas better tools to affect, in some areas less possibilities**	**At this point I suspect NIS should read: Network Information Security and not National Information Security**

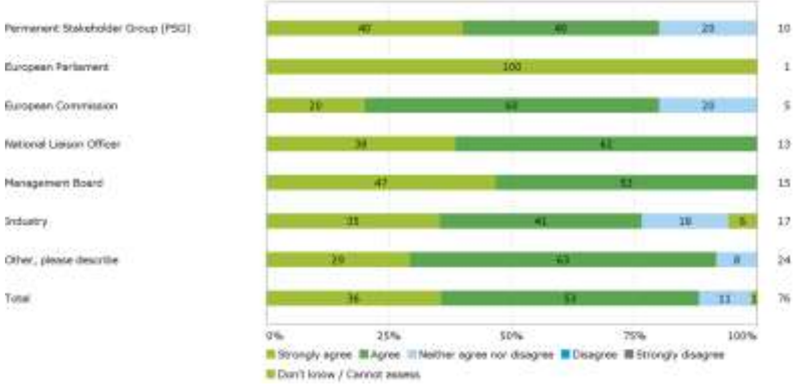
3. EFFECTIVENESS: SUPPORT TO CAPACITY BUILDING

3.1 Are you familiar with ENISA's work to support the capacity building of EU Member States and public and private sectors, as well as its efforts to contribute to raising the level of awareness of EU citizens?

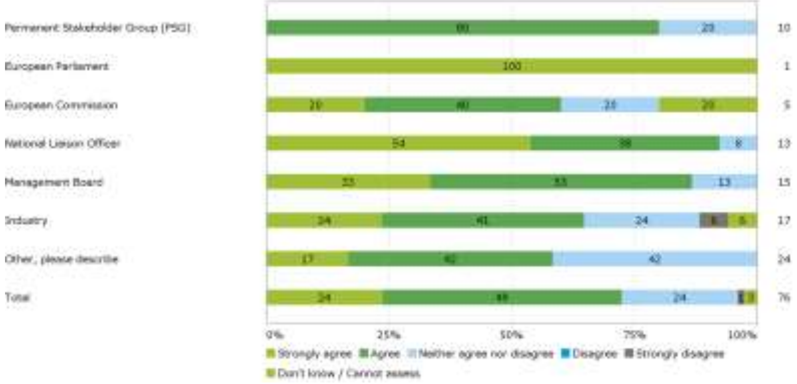


Please rate the extent to which you agree or disagree with the following statements concerning ENISA’s support to capacity building:

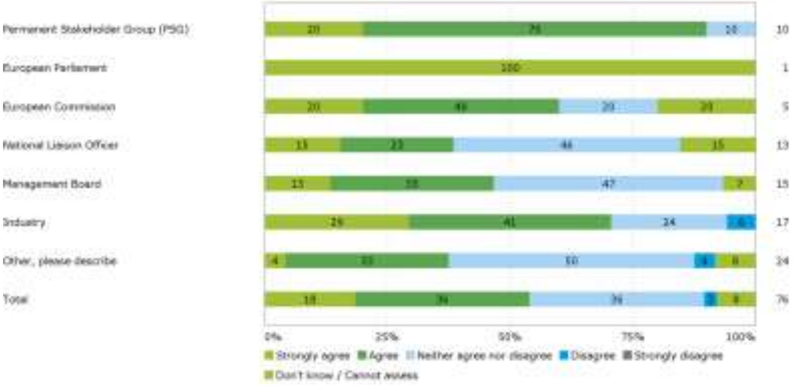
3.2 Good practices in NIS have been disseminated by ENISA



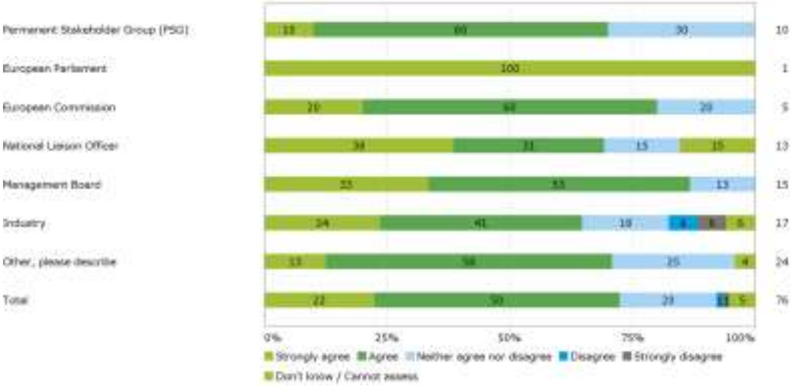
3.3 ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States



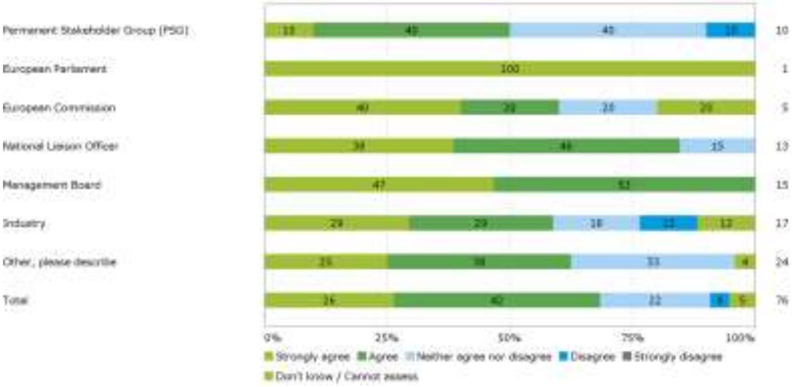
3.4 ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or incidents



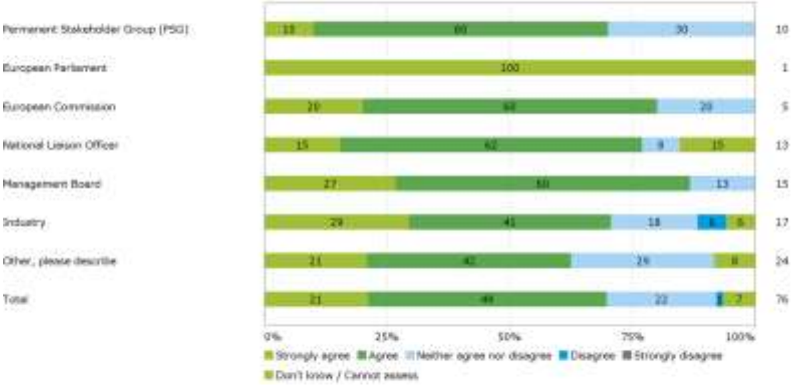
3.5 The support provided by ENISA in capacity building complements that of other public interventions



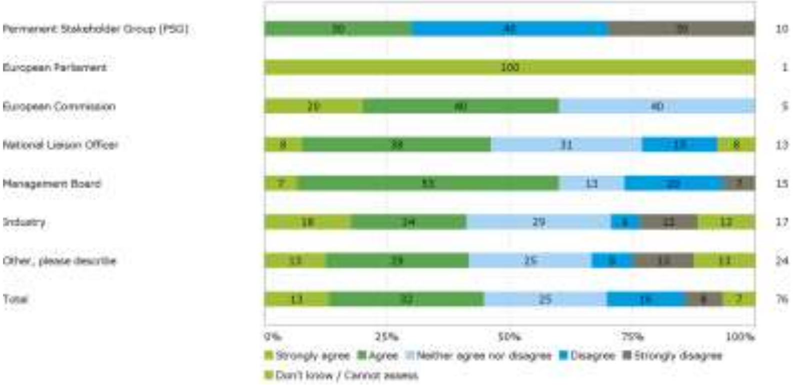
3.6 ENISA's support has enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis



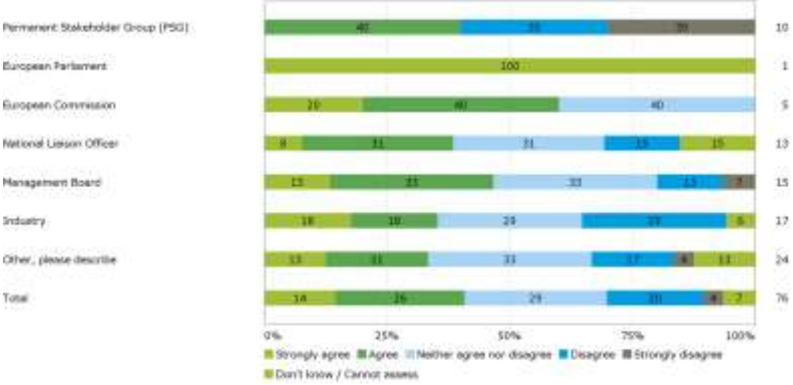
3.7 Sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA



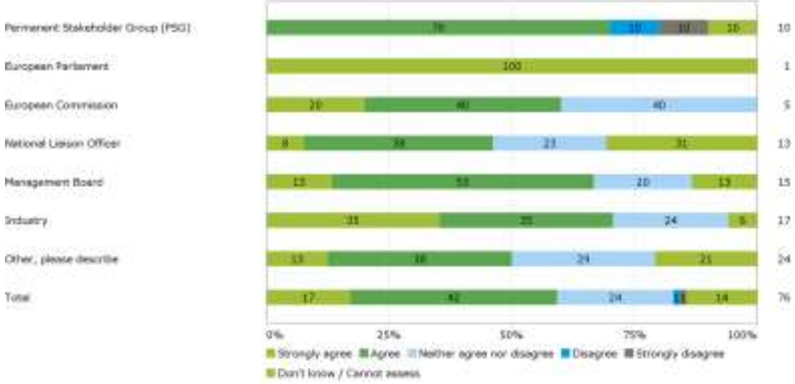
3.8 Cyber security challenges are adequately addressed in the EU



3.9 Cyber security challenges are adequately addressed in the Member States



3.10 ENISA's activities ensure adherence to EU Data Protection Legislation

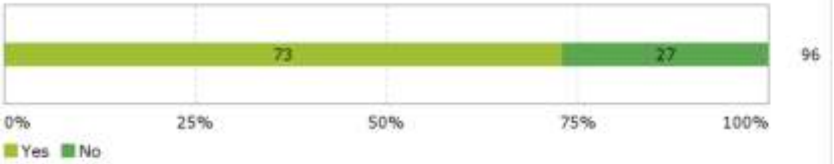


3.11 Please provide additional comments as relevant:

European Commission	Industry	Industry / Other	Permanent Stakeholder Group (PSG) / Management Board / Other	Other
• some of the questions are not well phrased, hence the ambivalent answers	• I think the output from ENISA is excellent. However, some member states ignore it, while ENISA is not known in the corporate space therefore the advise is lost.	• I think ENISA could do a lot more to promote and disseminate their material. When I mention ENISA in various meetings/conferences I often get blank stares as to who ENISA are. Also I suggest reviewing the navigation of the website to make it easier for visitors to find relevant information.	• ENISA's limited resources cannot compensate MS perhaps lack of competence	• ENISA has been good and relevant generating valuable information and awareness, though, lacks powers to enforce recommendations and capacity to play a coordinator role. • More effort needs to be taken to break through IT security biased polices which also address the cybersecurity of industrial control systems

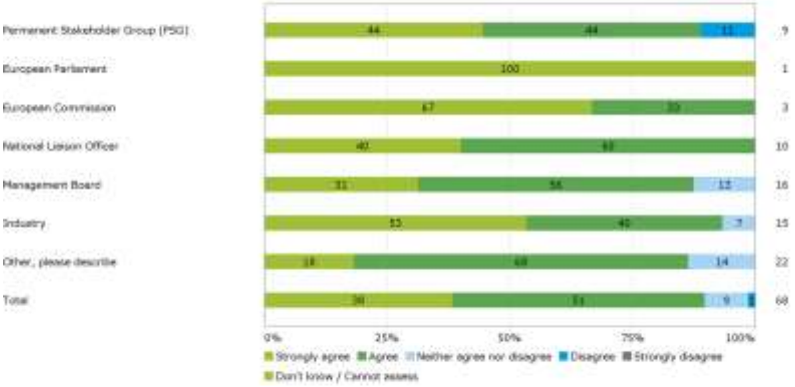
4. EFFECTIVENESS: SUPPORT COOPERATION

4.1 Are you familiar with ENISA's work to support cooperation between all stakeholders relevant and active in the area of NIS?

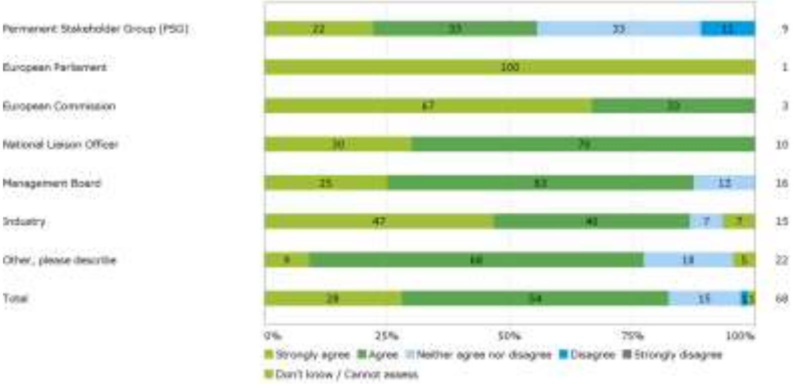


Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to cooperation:

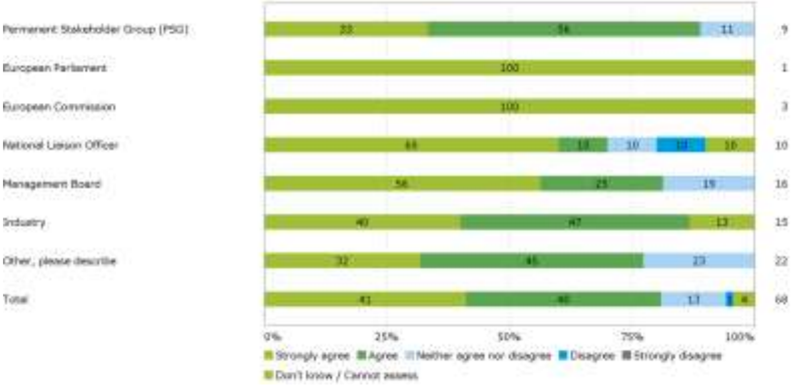
4.2 NISA effectively supports the sharing of information, ideas and common areas of interest among stakeholders



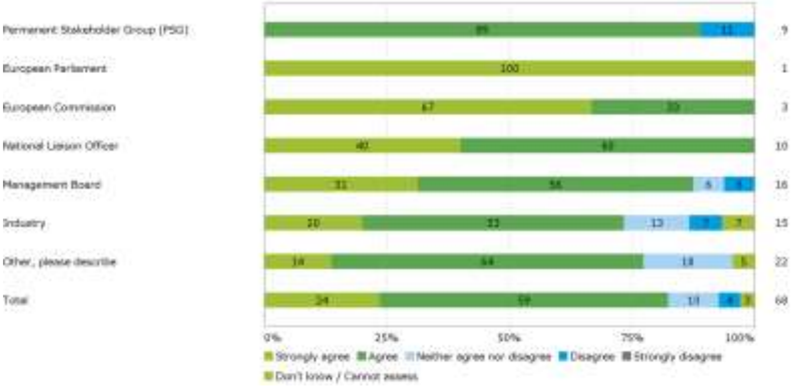
4.3 ENISA's support to cooperation between stakeholders complements other public interventions



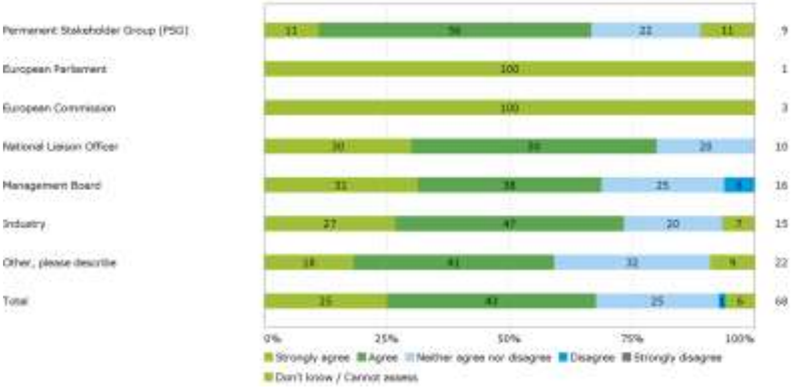
4.4 ENISA effectively shares lessons learned from cyber exercises with other communities and sectors



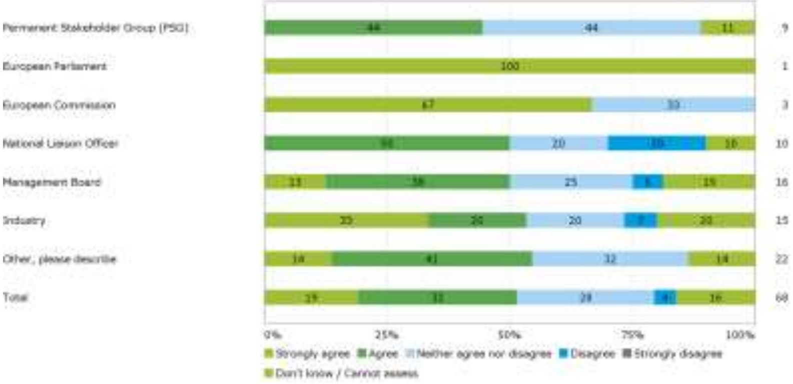
4.5 ENISA's support has contributed to enhanced cooperation in operational communities



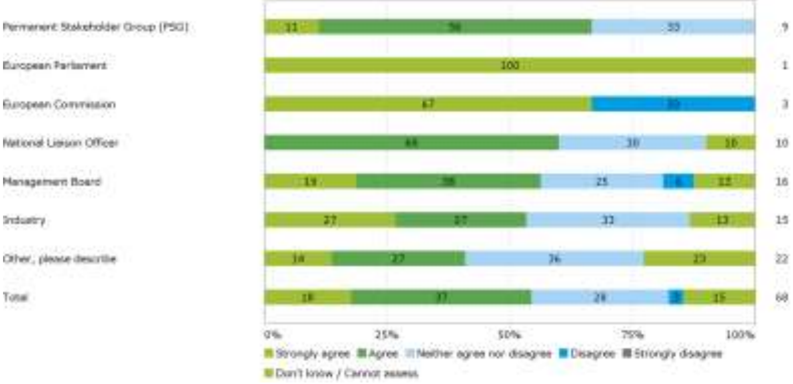
4.6 ENISA's support has improved services, workflow and communication among stakeholders to respond to crises



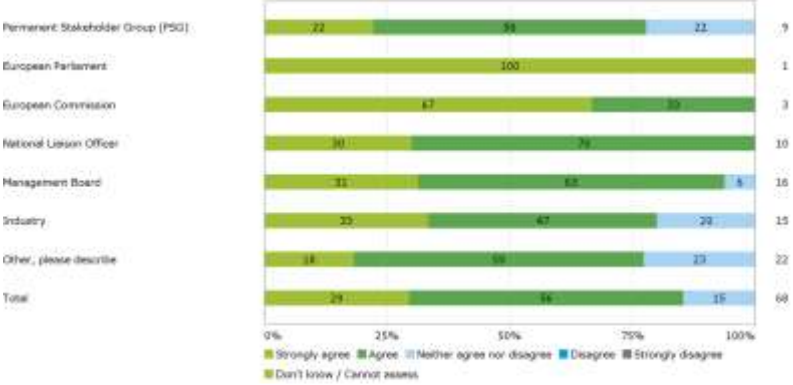
4.7 Technical capacity has increased among involved stakeholders



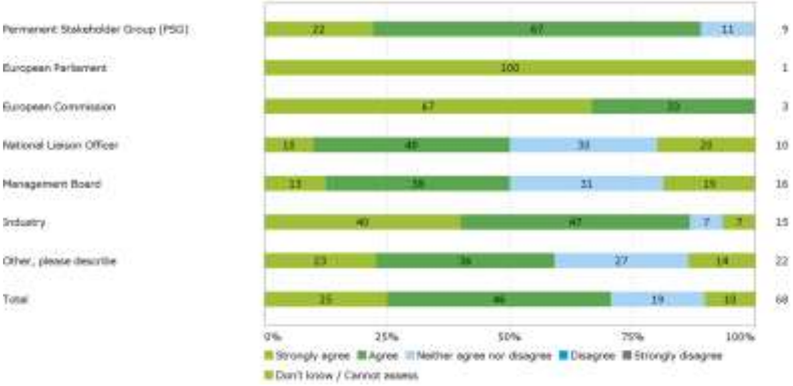
4.8 ENISA's support has enabled emergency mitigation and responses to be put in place at low resource and time costs



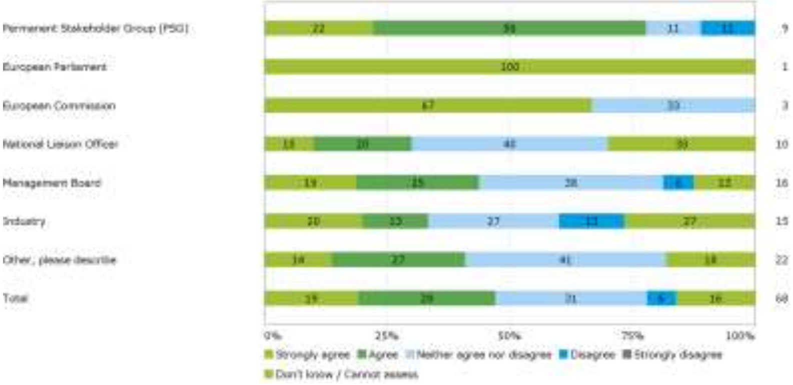
4.9 The support from ENISA has contributed to enhancing community building in Europe and beyond



4.10 ENISA supports the development and implementation of Data Protection and Privacy regulation



4.11 ENISA increases coherence between EU funded R & D projects and the objectives of NIS policy



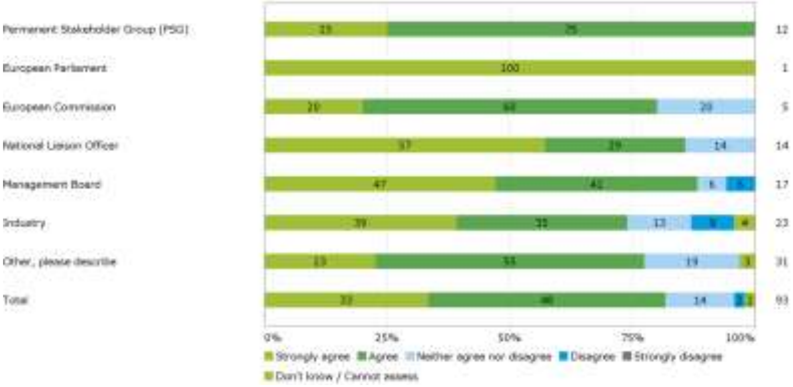
4.12 Please provide additional comments as relevant:

Permanent Stakeholder Group (PSG) / Management Board / Other	Other
• ENISA is already recognised player also outside EU	• ENISA has been good and relevant generating valuable information and awareness, though, lacks powers to enforce recommendations and capacity to play a coordinator role. • In order ENISA's support to cooperation between stakeholders complements other public interventions, these should be currently tracked down. • ENISA should be careful at not becoming bureaucratic and unreachable on a one on one basis

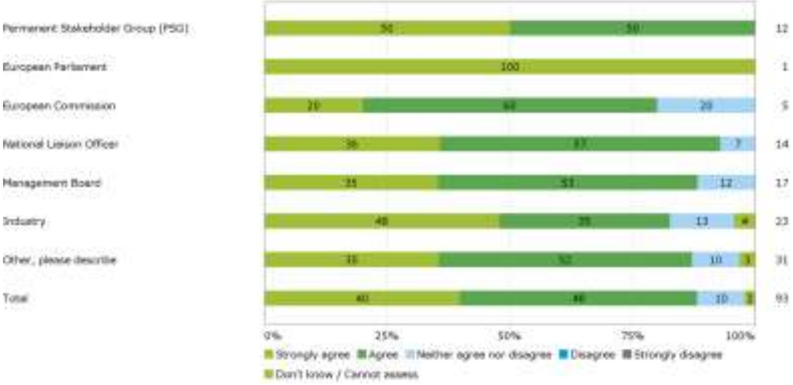
5. IMPACT OF ENISA'S SUPPORT

Please rate the extent to which you agree or disagree with the following statements concerning ENISA's contribution to its overall objectives:

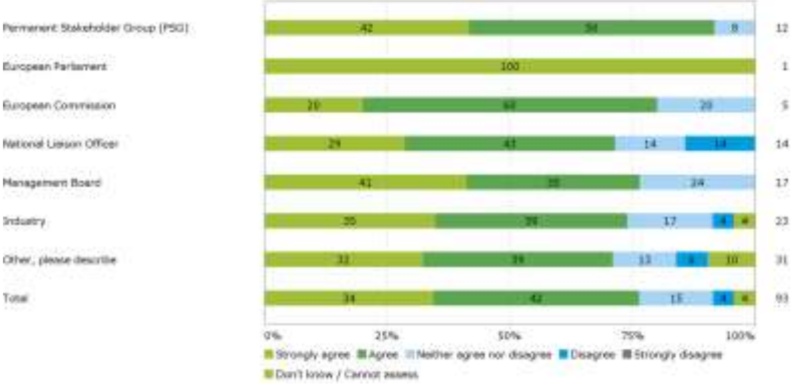
5.1 ENISA clearly contributes to ensuring a high level of NIS within the EU



5.2 ENISA clearly contributes to raising awareness of NIS within the EU



5.3 ENISA clearly contributes to promoting a culture of NIS in society



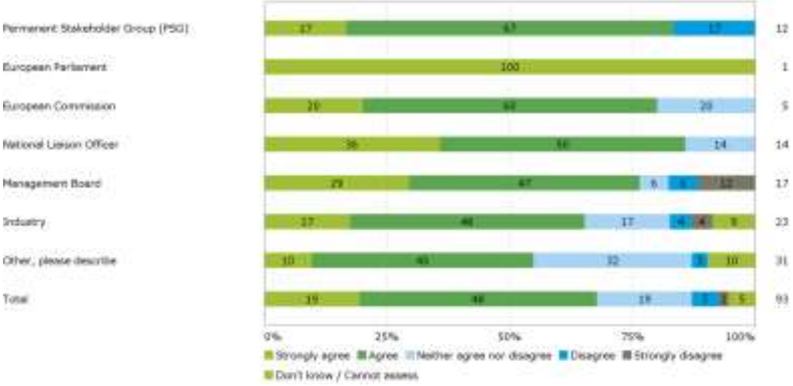
5.4 Please provide additional comments as relevant:

National Liaison Officer	National Liaison Officer / Other	Industry / Other	Permanent Stakeholder Group (PSG) / Management Board / Other	Other
• maybe more coordination needs to be invested in CERTs	• ENISA sie little known to people outside the NIS community.	• There is a better awareness of ENISA amongst government sector but still a lot of work to make ENISA more aware within the private sector	• ENISA is currently the best vehicle with NIS	• Direct access to general public is very difficult for EU agency • Needs to be complemented with work in industrial control systems as they relate to critical infrastructure

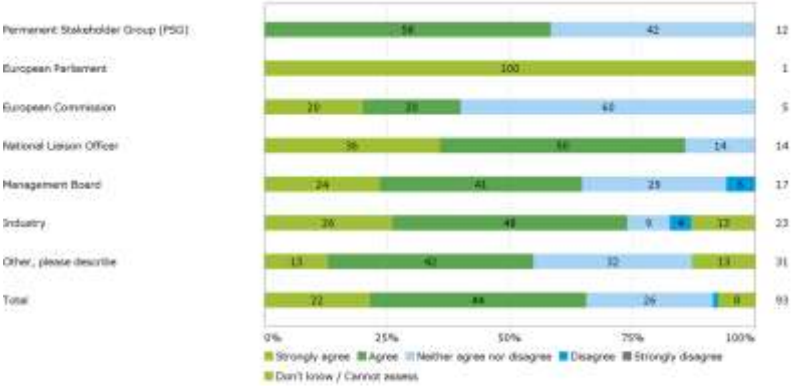
6. EU ADDED VALUE

Please rate the extent to which you agree or disagree with the following statements concerning ENISA:

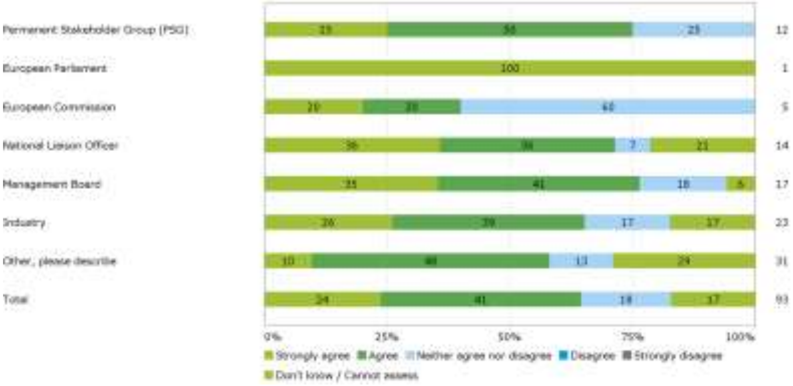
6.1 ENISA contributes with relevant and reliable information, which other sources do not provide



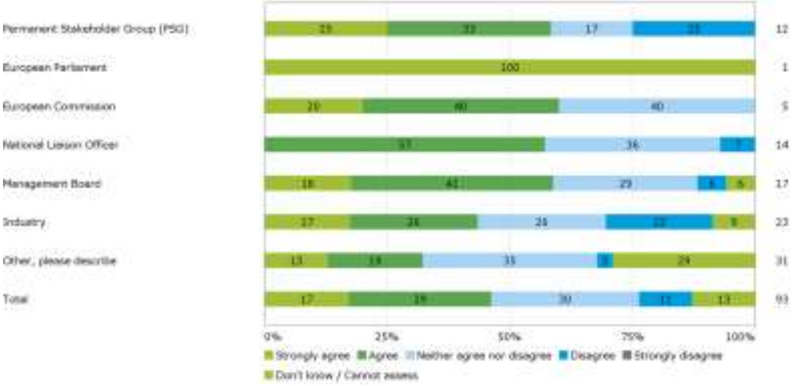
6.2 ENISA supports national actions in general



6.3 ENISA supports specific areas of national action



6.4 There are cases where ENISA activities duplicate efforts, because other similar initiatives are taking places



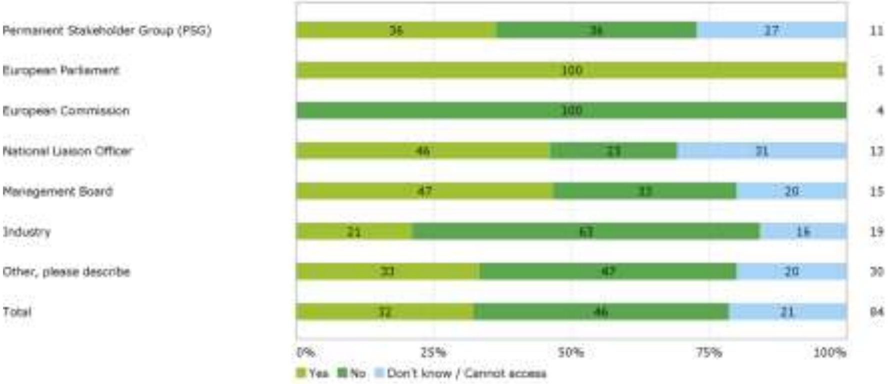
6.5 Please provide additional comments as relevant:

European Commission	Permanent Stakeholder Group (PSG) / Management Board / Other	Other
• The last question here is ambiguous, hence the answer	• Duplication is sometime coming while ENISA activities are copied	• ENISA has been supporting a couple of Member States

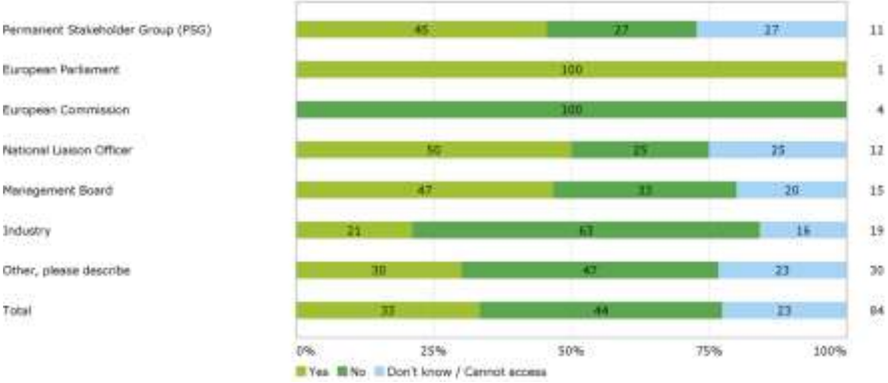
7. ADD ON TO THE GENERAL SURVEY

Have you made use of any ENISA publications which were published in 2015 or the workshop listed below? You will not be asked specific questions in relation to the publications or the workshop.

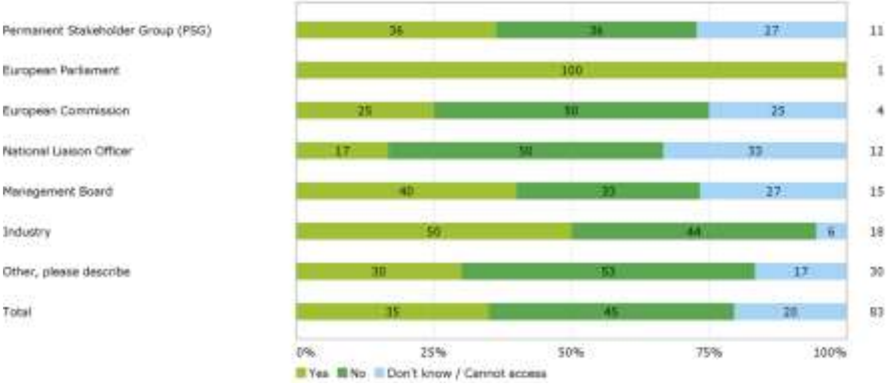
7.1 Stocktaking, Analysis and Recommendations on the Protection of CIIs



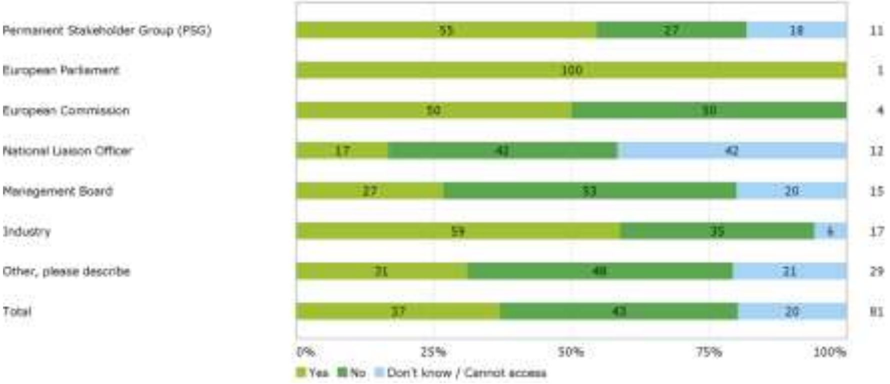
7.2 CIIP Governance in the European Union Member States" (Annex to "Stocktaking, Analysis and Recommendations on the Protection of CIIs")



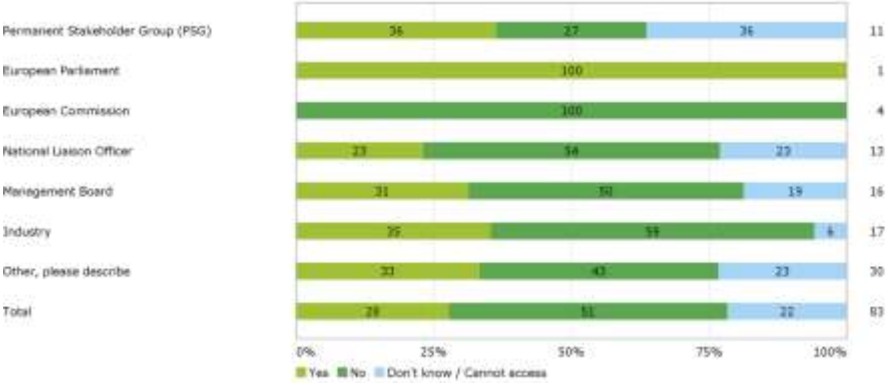
7.3 Methodology for the Identification of Critical Communication Networks, Links, and Components" (also known as "Communication network independencies in smart grids")



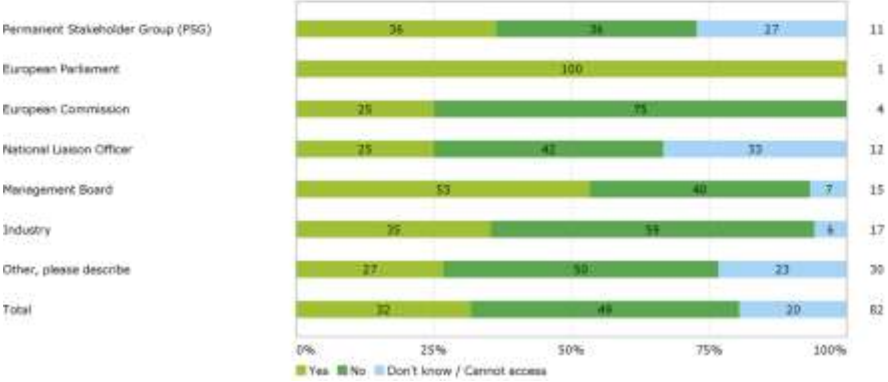
7.4 Secure Use of Cloud Computing in the Finance Sector. Good Practices and Recommendation



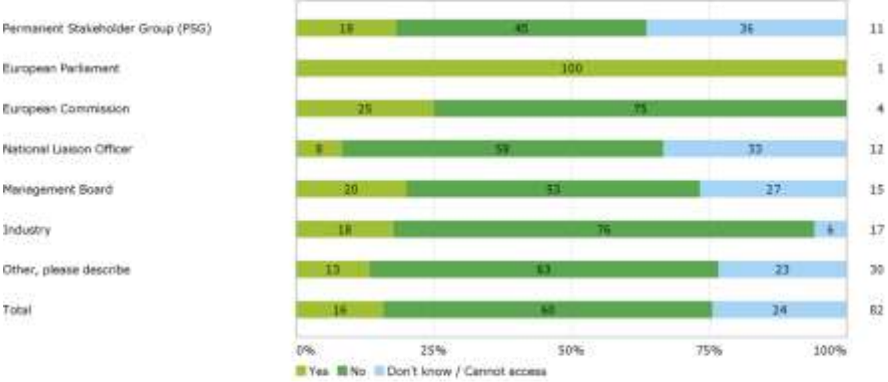
7.5 Security and Resilience in eHealth. Security Challenges and Risks



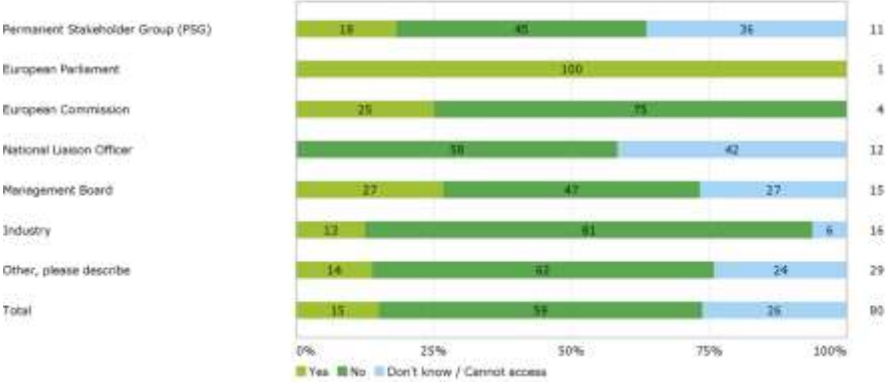
7.6 Mobile Threats Incident Handling. Handbook, Document for Teachers



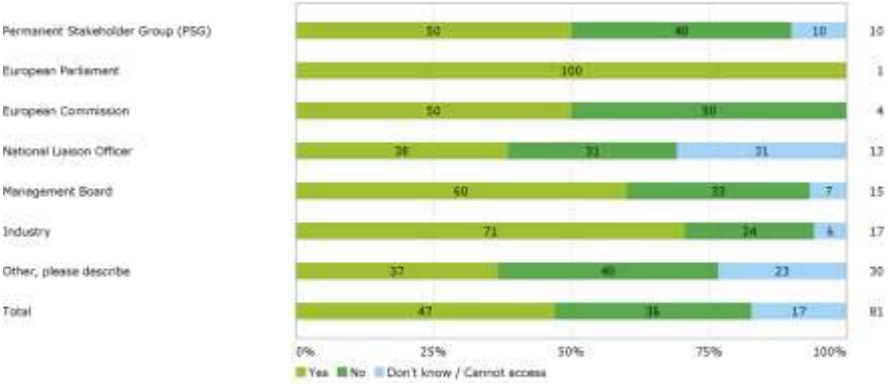
7.7 Advanced Dynamic Analysis. Handbook, Document for Teachers



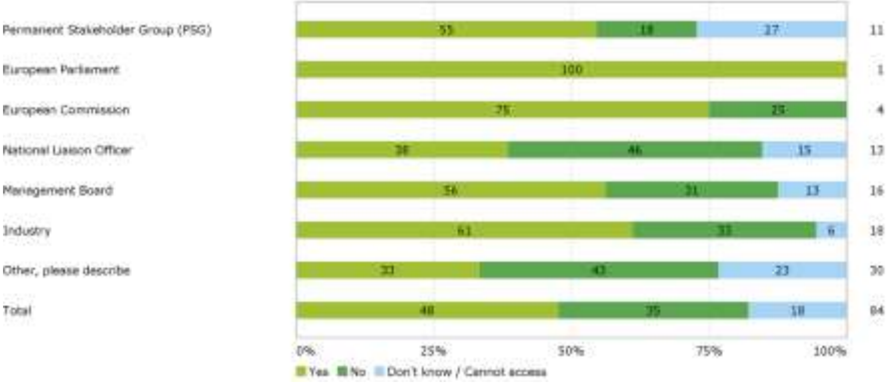
7.8 Advanced Static Analysis. Handbook, Document for Teachers



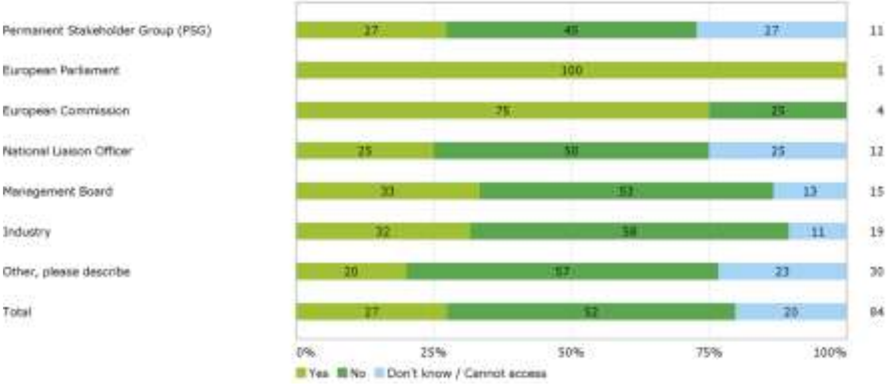
7.9 Good practice Guide on Vulnerability Disclosure. From Challenges to Recommendations



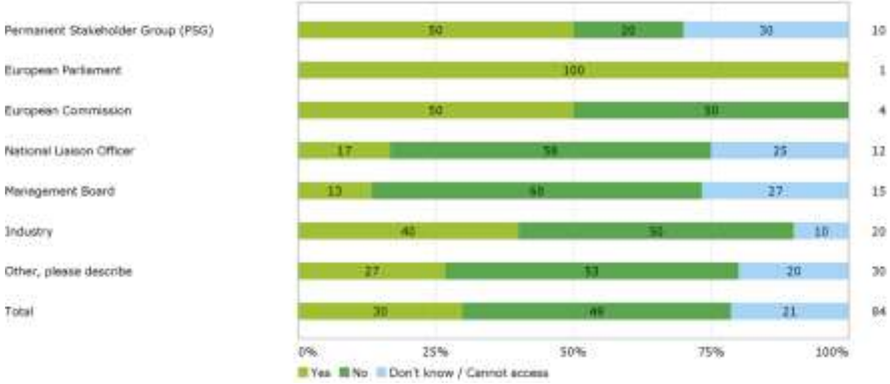
7.10 Leading the Way. ENISA's CSIRT-related Capacity Building Activities. Impact Analysis - Update 2015



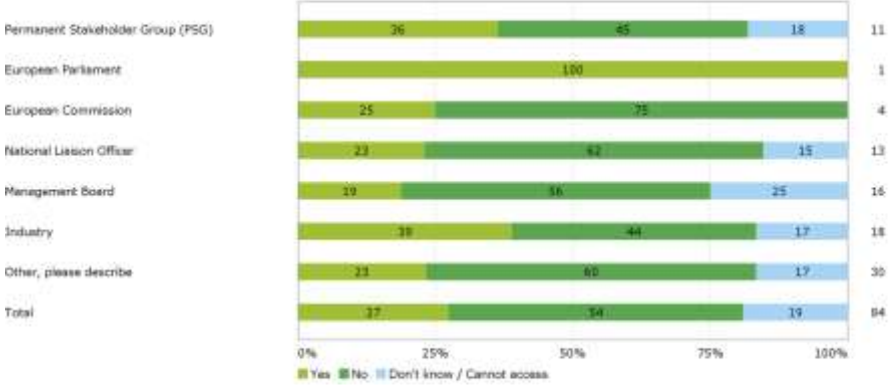
7.11 Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. Methodology, Pilot Assessment, and Continuity Plan



7.12 Privacy By Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics



7.13 Participated in the workshop "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA Event"

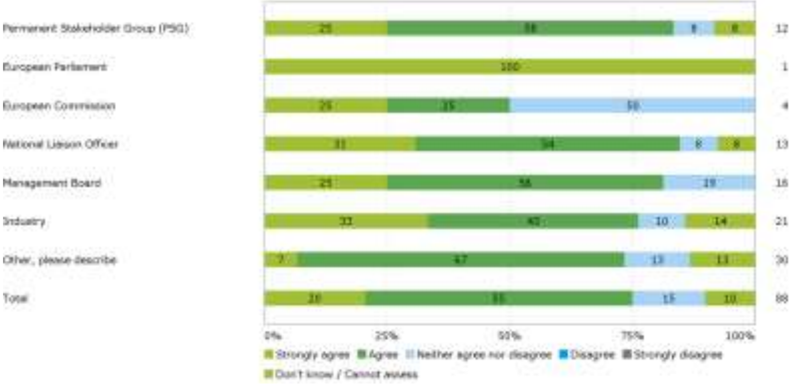


7.14 Please provide additional comments as relevant:

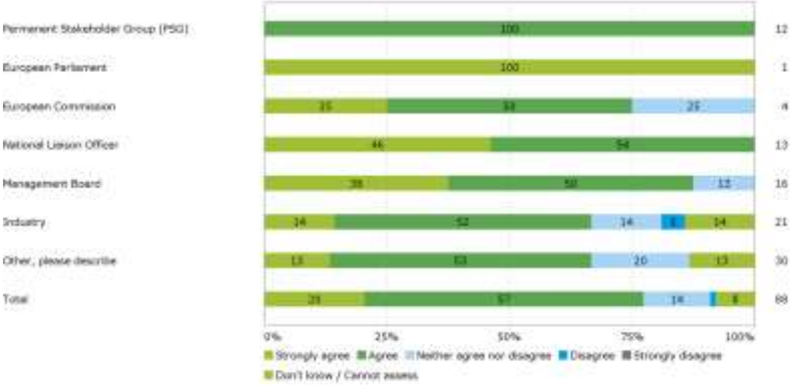
Industry	Other
• My experience of ENISA's output has been of consistent quality and timeliness of information distribution	• Only involved with Article 13a work

Please rate the extent to which you agree or disagree with the following statements concerning ENISA:

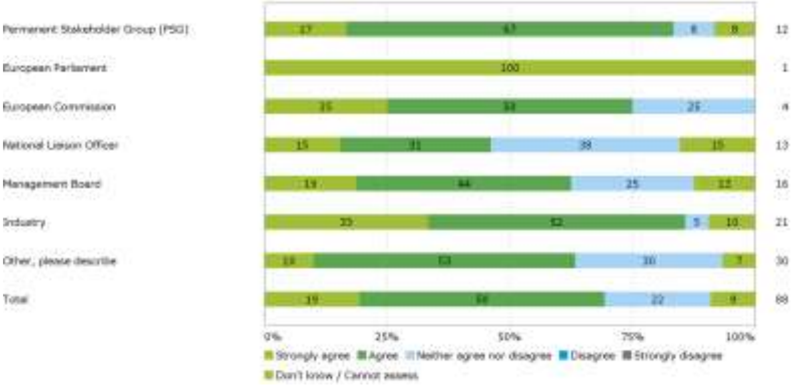
7.15 ENIAS's work, outputs and publications provide stakeholders of CII with advice and assistance



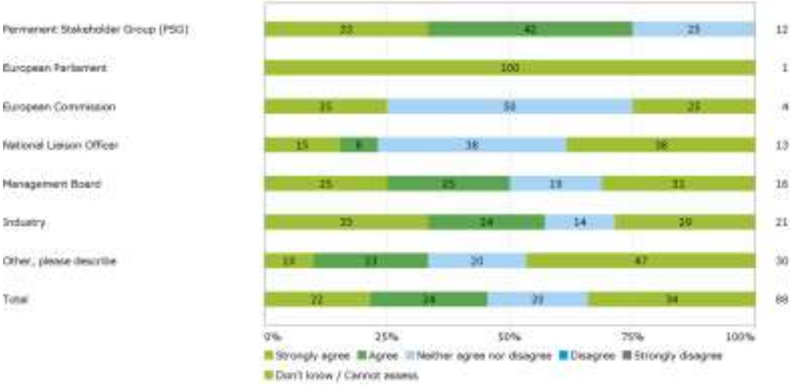
7.16 ENISA's work, outputs and publications help develop Member States' and the EU's ability to prevent, detect, analyse and respond to threats



7.17 ENISA's work, outputs and publications have supported the development and implementation of EU regulation in the area of data protection and privacy



7.18 ENISA's workshop on "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA event" has helped disseminate good practices regarding cyber security among private and public stakeholders



7.19 Do you have any particular suggestions as to how ENISA could improve in the future?

Permanent Stakeholder Group (PSG)	National Liaison Officer	Management Board	National Liaison Officer / Other	National Liaison Officer / Management Board
• The ENISA main office should be located in Brussels • Keep the good work • Less studies more practical examination of infrastructure protection measures	• Provide technical recommendations regarding algorithms in the area of eIDAS regulation as it is necessary in order to ensure interoperability and security of services. • No • Shorter response time and more reliability in handling national inquiries.	• sharing , communication and a better execution! • There is potential for ENISA to specifically address some of the obstacles that smaller, less resourced states face when implementing various NIS policies and procedures. These problems are often not encountered by larger EU states and can often go unrecognised in the debate around NIS.	• ENISA should focus more on using multipliers to spread its work. information	• Search for effective means to disseminate output from ENISA publications

Permanent Stakeholder Group (PSG) / Management Board / Other	Industry	Other
• ENISA need to have solid support from DG_Connect. Workload need to be realistic. ENISA is credible doer also outside EU, should this be somehow used?	• It would be useful to include the more finance sector participants in cyber exercises. It is also useful to include European but non-EU countries such as Switzerland for participation in initiatives. • Some work is a little more consensus based, and less practical than it could be. For some things this is good, but for some subjects, clearer concise technical reports are needed. Over all very happy, but we could be a little more bold in R&D. • Enhancing its role of coordination of private stakeholders' standpoints towards new EU regulations (before their approval). • We need to think about how ENISA's work can reach a wider audience. • No, I have only positive impressions of their work and outreach. • develop robustness certification of products and services	• ENISA needs to take on a more proactive role and also move from paper-work support to ad-hoc, more practical support or even coordination • More interactivity between ENISA and stakeholders, especially in National Level. • Communicate, create a network, ISAC engage stakeholders • Focus on coming up with lessons learned regarding real world cyber incidents. Use the cyber attacks on Ukraine's electric power grid which took place on December 23, 2015 as an object of study. Lessons learned can be used to improve the cybersecurity of both Ukraine and EU member states. • Mailing list for the general public

APPENDIX 6
DOWNLOADS OF PUBLICATIONS - 2014 CORE OPERATIONAL ACTIVITIES

As part of this year's evaluation, we took a more in-depth look at the download rates of ENISA's 2014 publications above the value of €30,000 (see Table 28 below), in order to develop a firmer baseline regarding downloads for the future evaluations than was included in the evaluation of ENISA conducted in 2014 (presented in the final report). It was not possible to conduct a similar analysis of the publications from 2015, since some of these only came online recently (in 2016), which would not give an accurate picture of the downloads of these publications; they will be analysed in next year's evaluation.

Table 28 ENISA publications from 2014 Work Programme[114]

Work package[115]	Deliverable (No.)	Title of the publication
		SO1
WPK 1.1	D1	ENISA Threat Landscape 2014
	D2	Threat Landscape and good practice guide for smart home and converged media;
		Threat Landscape and good practice guide for Internet infrastructures
WPK 1.2	D3	Algorithms, key size and parameters report 2014
		Study on cryptographic protocols
WPK 1.3	D1	Standardisation in the field of Electronic Identities and Trust Service Providers
		SO2
WPK 2.1	D2	An evaluation framework for Cyber Security Strategies
	D5	Developing countermeasures
		Common framework for artefact analyses activities
		Advanced artefact handling
		Processing and storing artefacts
		Building an artefact handling and analyses environment
	D6	Impact assessment and roadmap
WPK 2.2	D2	Smart grid security certification in Europe
	D3	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts
	D5	Cloud security guide for SMEs

[114] This list is in accordance with Annex A of the Final report for the external evaluation of ENISA´s activities conducted in 2015. Please note that only WPK´s with deliverables that have budgets exceeding €30.000 are listed.

Work package[115]	Deliverable (No.)	Title of the publication
	D6	Security framework for governmental clouds
	D7	Methodologies for the identification of critical information infrastructure assets and services
	D8	Network and Information Security in the Finance Sector — Regulatory landscape and Industry priorities
		SO3
WPK 3.1	D2	Report on Cyber Crisis Cooperation and Management
WPK 3.2	D1	Annual Incidents report 2013
		Technical Guideline on Incident Reporting V2.1
		Technical Guideline on Security Measures V2.0
		Secure ICT Procurement in Electronic Communications
		Security Guide for ICT Procurement; Protection of underground electronic communications infrastructure
WPK 3.3	D2	Best practice guide on exchange processing of actionable information — exercise material
	D3	Stocktaking of standards formats used in exchange of processing actionable information

The subsequent sections of this annex include:

- A description of the methodology employed for the descriptive analysis if the download statistics
- An overall analysis of deliverables across WPKs
- An analysis by WPK

Drawing on this revised data, an updated version of the table presented in last year's final report, including details of costs per download is presented in Appendix 8. The aggregate data is presented in Appendix 7.

7.20 Methodology for the descriptive analysis of the download statistics

The descriptive analysis of download statistics for the 2014 deliverables has been carried out on the basis of data sets extracted from Google Analytics containing four elements: source, medium, country, and number of downloads[116]. The data does not include traffic made by ENISA's web developer or Webmaster, but may include downloads generated by ENISA staff[117].

Key elements of the descriptive analysis

The focus of the analysis has been to examine the volume of downloads of deliverables, and examine the distribution of overall downloads in the EU. In addition, the analysis has included figures on how users get to the page where they download the publications, the so-called "mediums". The table below provides an overview of the four mediums included in the analysis.

Table 29 Explanation of the four different Mediums

Medium	Explanation
Referral	The recipient has arrived to the publication by clicking on a link on another website/email.
Organic	Organic traffic is all the traffic that comes from unpaid sources on search engines

[116] ENISA has not enabled the feature for gathering demographic information (e.g. age, gender, interests) of its users as this would mean enabling Google Analytics Advertising Features which would be against the Agency´s privacy policy.

[117] It was not possible for ENISA to exclude all ENISA IP addresses in the data provided to Ramboll. However, the Agency assessed that this does not compromise the data accuracy and that internal downloads are minimum as the publications are also stored in ENISA´s internal (intranet) libraries. Our analysis of the data substantiated this view in that as a general rule, downloads from "Greece" remained low in comparison to the totals.

Medium	Explanation
	like Google, Yahoo and Bing.
None	In a high number of cases Google Analytics cannot determine the referrer who brought the users to the page where he/she downloaded an ENISA publication. Thus, this medium, "none", does not provide explanatory power in determining how users found the publication, since it can cover a variety of instances, including the two most common which are clicking a link from an email or clicking a link from a Microsoft Office or PDF document[118].
Other	This medium is only reported as used very rarely and covers instances similar to the medium "referral", but which in the data set specifically refers to the social media sites, and in particular twitter.

The data on "sources" was not included in the analysis for two key reasons. Firstly, the form of the data did not allow for a valid analysis due to the high variety of entries of which a share were not easily identifiable (as a search engine, web page etc.) and thus not meaningful. Secondly, for all deliverables the majority of sources were categorised as "direct", which occurs any time Google Analytics cannot determine another referrer. This means that it was not possible to draw valid conclusions in relation to sources on the basis of the data available.

Time scope[119]

The descriptive analysis covers the download of publications between September 1st 2014 and December 31st 2015, depending on when a document was made public and ready for download. Further details on the period covered for each deliverable can be found in the sub-sections covering the individual Work Packages. Please note that the time scope for each publication covers the publication date, but that it may also include some days before the publication. This is due to the filter used to extract the data from Google Analytics, which may cover a broader period of time.

Geographical scope

In line with the geographical scope of the evaluation of ENISA, this analysis covers the EU Member States. However, in certain cases, reference is made to third countries where relevant for the analysis.

7.21 Overall analysis of deliverables across WPKs

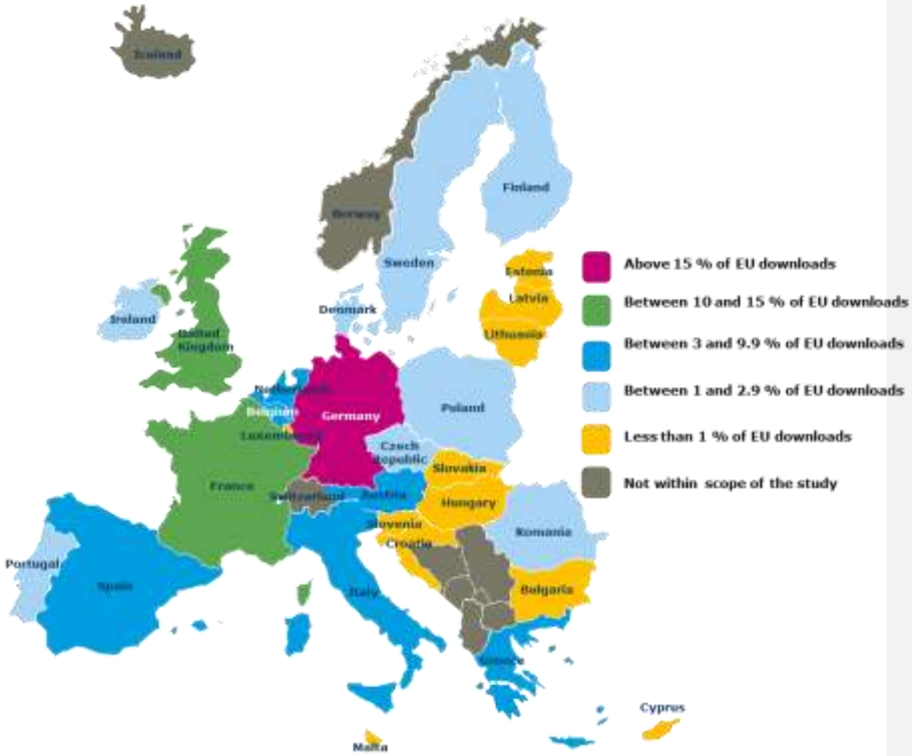
In total, the deliverables which were subject to this analysis, were downloaded 154,891 times across the globe, and of which 46% (71,338) were within the EU, and for 2% (3,313) downloads the web-statistics could not identify the location of the user.

The distribution of downloads differs across the EU and the size of a Member State is likely to be an influencing factor.

[118] Other instances include: Accessing the site from a shortened URL (depending on the URL shortener); clicking a link from a Mobile social media apps like Facebook or Twitter (phone apps often do not pass referrer information); going to a non-secure (http) site from a link on a secure (https) site, as the secure site will not pass a referrer to the non-secure site; and accessing a site from organic search, in some instances, will end up being reported as Direct due to browser issues.

[119] While for comparability purposes one could argue that it would have been better to cover the downloads of each deliverable for a period of a year after publication, such analysis would not have been possible with the resources at the team's disposal and would not have necessarily added much value to the analysis as a number of other factors (e.g. intended target audience) influence the number of downloads of a given publication.

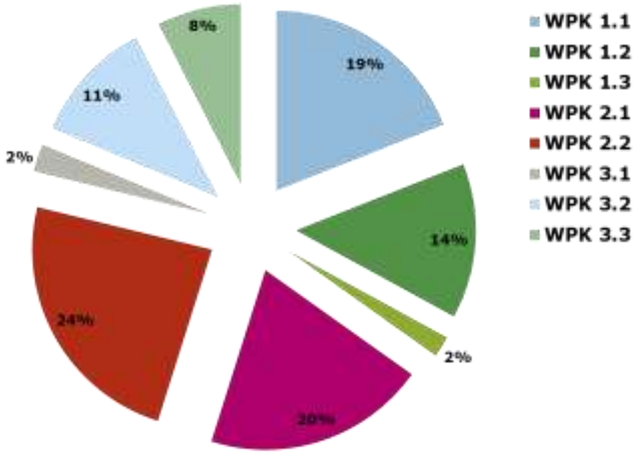
Figure 49 Distribution of downloads across the EU



As illustrated in the figure above, by far the most downloads were made in Germany, which accounts for 21% (15.229) of all downloads, followed by the United Kingdom accounting for 12% (8.990) and France at 11% (8.072). The fewest downloads occurred in Cyprus 0.16% (118), Malta 0.18 (135) and Latvia 0.3% (243). A full overview of downloads per country by WPK, deliverable and publication can be found in Appendix 6.

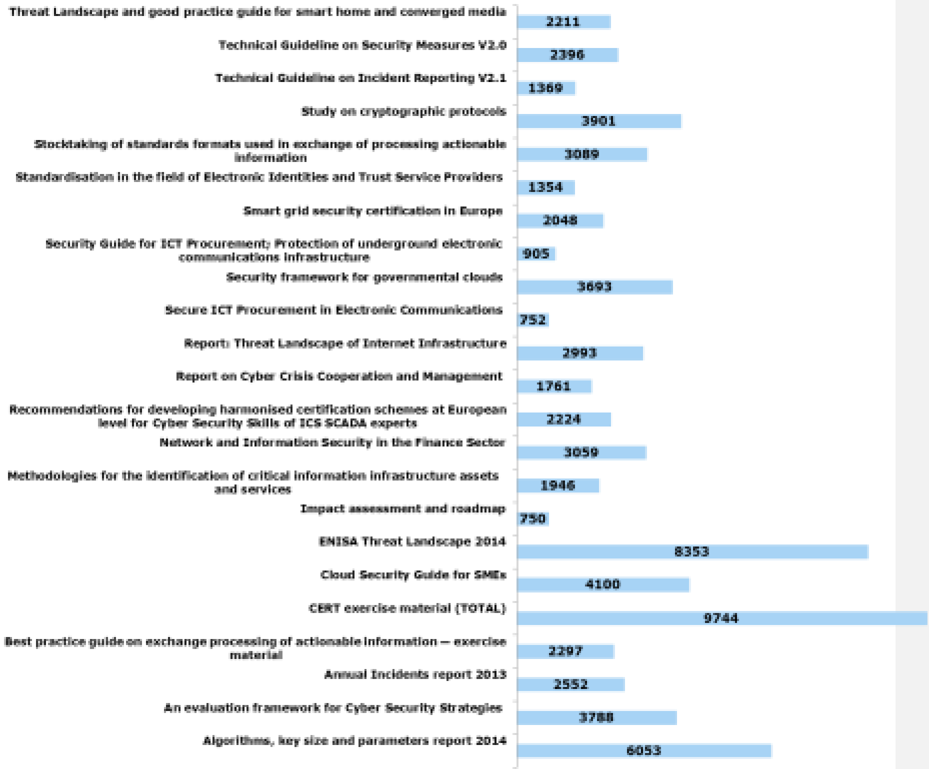
The deliverables under each Work Package were downloaded to different extents, which may be justified by the number of publications, the size of the target audience (covering the scope and purpose) of the specific deliverables.

Figure 50 Distribution of EU views across Work Packages



While the volume of downloads certainly testifies to the popularity and general usefulness of a deliverable, it is important to note that other factors may weigh in as well. Certain deliverables may therefore be downloaded less often, for example, if they are aimed at a smaller, highly specialised audience, or have restricted access. It is therefore not possible to conclude on the usefulness or importance of given deliverables exclusively on the basis of the download statistics.

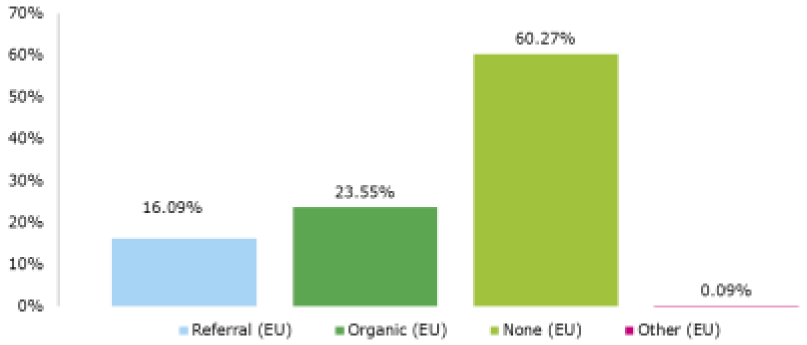
Figure 51 Total views within the EU by deliverable



Based on the statistics, it is difficult to conclude on which mediums (see Table 29) users use to get to the deliverables, since Google Analytics cannot determine who the referrer or source is in a majority of cases.[120]

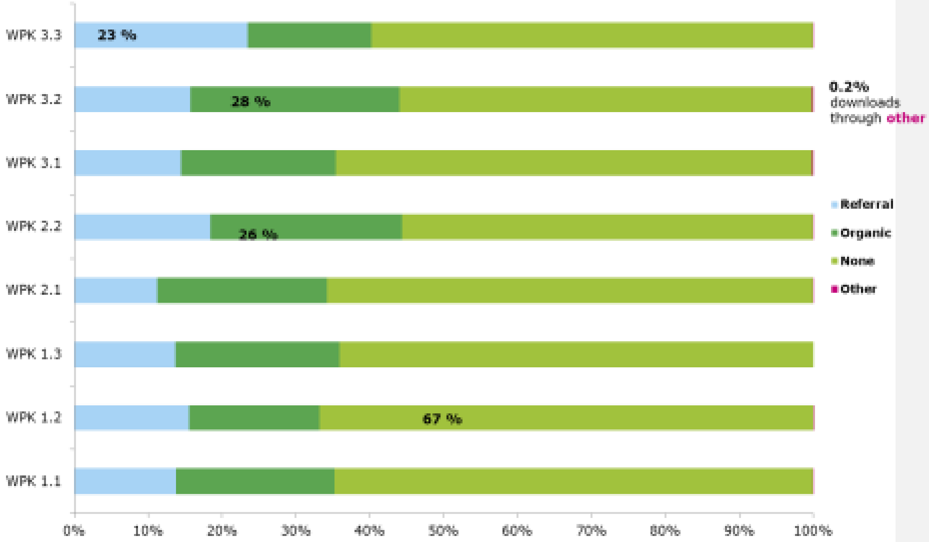
[120] For an explanation of the terms "referral", "organic", "non" and "other" please see section 3.1 explaining the methodology behind the descriptive analysis.

Figure 52 Average use of medium



At the same time, certain Work Packages, namely 2.2, 3.2, and 3.3, stand out from this pattern, as shown in the figure below, meaning that users access downloads in different ways.

Figure 53 WPK outliers in terms of the medium used



The following subsections provide further details on these Work Packages and highlight publications which are outliers in terms of the mediums used.

7.22 Work Package 1.1

In this section, download statistics for the following three deliverables under WPK 1.1 are presented:

- D1: ENISA Threat Landscape 2014
- D2: Threat Landscape and good practice guide for smart home and converged media
- D2: Threat Landscape and good practice guide for Internet infrastructures

Overall, these deliverables under WPK 1.1 were downloaded 13,557 times (out of a total across WPKs of 71,338 downloads within the EU) equalling 19 % of all views of all deliverables within the EU. The table below shows the key figures from the analysis of these downloads. The publication "ENISA Threat Landscape" contributed significantly to this, and based on the high volume of downloads, appears to have been relevant to a broad group of ENISA stakeholders. Thereby, the publication met the expectations set out in ENISA´s 2014 Annual activity report.

Table 30 Overview of downloads for WPK 1.1

	WPK 1.1 total	D1 ENISA Threat Landscape 2014	D2 Threat Landscape and good practice guide for smart home and converged media	D2 Threat Landscape and good practice guide for Internet infrastructures
Total views	27,684	17,459	4,722	5,503
Total EU views	13,557	8,353	2,211	2,993
Time scope of data	01.01.2015-31.12.2015	01.01.2015-31.12.2015	01.01.2015-31.12.2015	01.01.2015-31.12.2015

On the basis of the statistics provided, it is generally difficult to conclude on how a majority of users found the ENISA deliverables under WPK 1.1, since the statistics, on average (across the three deliverables), do not report a medium for 64.7% of the views; 21.4% of the downloads were generated by organic searchers and 13.8% by referral.

7.23 Work Package 1.2

In this section, download statistics for WPK 1.2´s deliverable 3 (D3) are presented for two publications, namely:

- D3: Algorithms, key size and parameters report 2014
- D3: Study on cryptographic protocols

In total these deliverables were downloaded 9,954 times in the EU (out of a total 20.682[121] downloads of those publications world-wide). Comparatively speaking the D3 deliverables under WPK 1.2 represents 14 % of all ENISA downloads in the EU.

Table 31 Overview of downloads for WPK 1.2

	WPK 1.2 total	D3 Algorithms, key size and parameters report 2014	D3 Study on cryptographic protocols
Total views	20,682	12,344	8,338
Total EU views	9,954	6,053	3,901
Time scope of data	01.09.2014-31.12.2015	01.09.2014-31.12.2015	01.09.2014-31.12.2015

On the basis of the statistics provided, it is generally difficult to conclude on how a majority of users found the ENISA deliverables under WPK 1.2, since the statistics, on average (across the three deliverables), do not report a medium for 67.3% of the views; 16.5% of the downloads were generated by organic searchers and 16.2% by referral (for the publication "Algorithms, key size and parameters report 2014", 0.02% (1 download) was made using twitter as the medium).

7.24 Work Package 1.3

Deliverable D1 for WPK 1.3 was the publication titled "Standardisation in the field of Electronic Identities and Trust Service Providers", which was downloaded 1,354 within the EU (out of a total 2,374 downloads globally).

[121] This figure includes 625 downloads were it was not possible to identify the location of the user.

Table 32 Overview of downloads for WPK 1.3

	WPK 1.3 total/D1 Standardisation in the field of Electronic Identities and Trust Service Providers
Total views	2,374
Total EU views	1,354
Time scope of data	01.01.2015-31.12.2015

In terms of the mediums used to locate the publication for download, the medium is not captured by 64.1% of the downloads, while 22.2% are generated by organic searches and 13.7% through referrals.

7.25 Work package 2.1

Work package 2.1 covers three deliverables, and seven publications:

- D2: An evaluation framework for Cyber Security Strategies
- D5: CERT Exercise Material
    - D5: Developing countermeasures
    - D5: Common framework for artefact analyses activities
    - D5: Advanced artefact handling
    - D5: Processing and storing artefacts
    - D5: Building an artefact handling and analyses environment
- D6: Impact assessment and roadmap

In total these deliverables were downloaded 14,282 times within the EU (out of a total of 32,348 downloads), making the deliverables under WPK 2.1 the second most downloaded among all eight work packages examined.

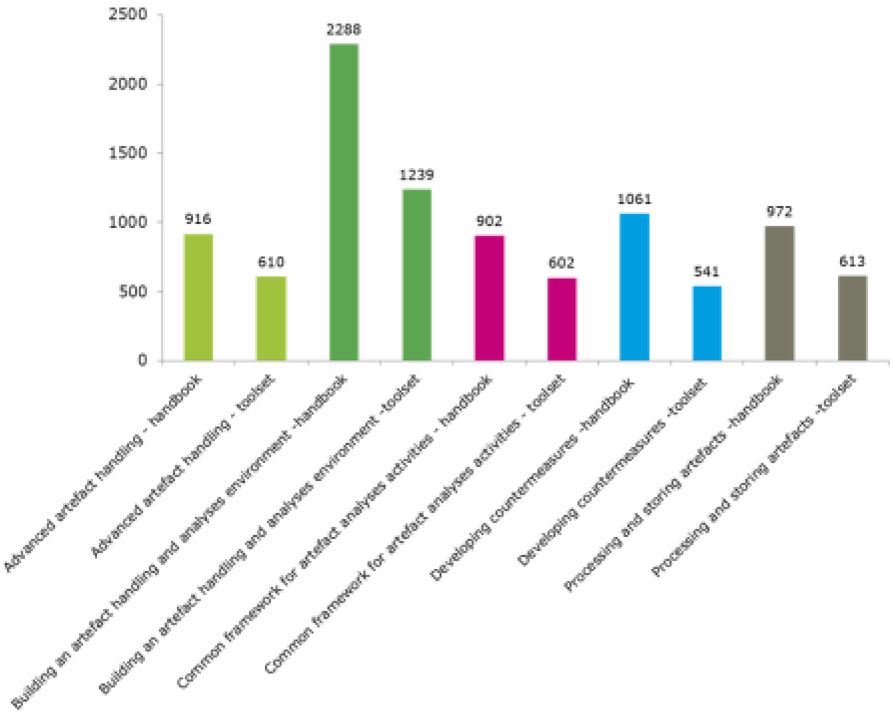
Table 33 Overview of downloads for WPK 2.1

	WPK 2.1 total	D2 An evaluation framework for Cyber Security Strategies	D5 CERT Exercise material	D6 Impact assessment and roadmap
Total views	32,348	14,792	16,159	1,397
Total EU views	14,282	3,788	9,744	750
Time scope of data	N/A	01.01.2015-31.12.2015	01.12.2014/20.12.2014-31.12.2015	01.12.2014-31.12.2015

In large part, the high volume of downloads of WPK 2.1 publications is explained by the deliverable D5 which contains the Cert Exercise material which in the period was downloaded 9,744 times, thus accounting for 68 % of all EU downloads of WPK 2.1 publications. D5 consists of the five publications shown in the bullet points above. For each one of these, both a handbook and a toolset is available. As shown in the overview below, the handbook for "Building an artifact handling and analyses environment" is the most downloaded, followed by the toolset for the same publication.

The pillars below are shown in pairs of one handbook and one tool-set, illustrated by using different colours.

Figure 54 Break down of publications under D5



Finally, it is worth noting that the publication "An evaluation framework for Cyber Security Strategies" (D2) was downloaded at a high rate globally (14,792 downloads including EU downloads), but that only 25% of these were within the EU. Most notably, the publication has been downloaded 5,345 times in the USA.

7.26 Work package 2.2

The analysis of the download statistics for WPK 2.2 covers six publications, namely:

- D2: Smart grid security certification in Europe
- D3: Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts
- D5: Cloud security guide for SMEs
- D6: Security framework for governmental clouds
- D7: Methodologies for the identification of critical information infrastructure assets
- and services
- D8: Network and Information Security in the Finance Sector — Regulatory landscape and Industry priorities

In total, these deliverables were downloaded 17,070 times in the EU (out of 37,174 downloads of WPK 2.2 publications world-wide), making it the WPK with the most downloads.

Table 34 Overview of downloads for WPK 2.2

	WPK 2.2 total	D2 Smart grid security certification in Europe	D3 Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts	D5 Cloud security guide for SMEs	D6 Security framework for governmental clouds	D7 Methodologies for the identification of critical information infrastructure assets and services	D8 Network and Information Security in the Finance Sector — Regulatory landscape and Industry priorities
Total views	37,174	3,185	5,042	11,429	7,850	3,297	6,371
Total EU views	17,070	2,048	2,224	4,100	3,693	1,946	3059
Time scope of data	N/A	01.12.2014-31.12.2015	01.01.2015-31.12.2015	01.01.2015-31.12.2015	01.01.2015-31.12.2015	01.01.2015-31.12.2015	01.01.2015-31.12.2015

In 55.6% of cases, the medium cannot be determined, while 26.0% were generated by organic searches, and 18.4% by referral. In terms of the medium used, WPK 2.2 deviates from the average (taken from all WPKs and shown in section 7.21 above) since a fourth of all downloads are generated by organic sources, which is exemplified by the D7 "Methodologies for the identification of critical information infrastructure assets and services", where more than 35% of downloads were facilitated by such sources. Another publication which can be described as an outlier is D6 ”Security framework for governmental clouds", where 30% of downloads were achieved through referral.

7.27 Work Package 3.1

Deliverable D2 for WPK 3.1 was the publication "Report on Cyber Crisis Cooperation and Management", which was viewed 1,761 within the EU (out of a total 2,652 views globally).

Table 35 Overview of downloads for WPK 3.1

	WPK 3.1 total D2 Report on Cyber Crisis Cooperation and Management
Total views	2,652
Total EU views	1,761
Time scope of data	01.09.2014-31.12.2015

In terms of the mediums used to locate the publication for download, the medium is not captured in 64.5% of the downloads, while 20.9% are generated by organic searches, 14.4% through referrals, and 0.2% through twitter (three downloads in France and Belgium).

7.28 Work Package 3.2

Under WPK 3.2 one deliverable was examined, namely D1 which contains the following five publications:

- D1: Annual Incidents report 2013
- D1: Technical Guideline on Incident Reporting V2.1
- D1: Technical Guideline on Security Measures V2.0
- D1: Secure ICT Procurement in Electronic Communications
- D1: Security Guide for ICT Procurement; Protection of underground electronic communications infrastructure

In total, these publications under WPK 3.2 were downloaded 7,974 times within the EU (out of 17,017 globally).

Table 36 Overview of downloads for WPK 3.2

	WPK 3.2 total	D2 Annual Incidents report 2013	D1 Technical Guideline on Incident Reporting V2.1	D1 Technical Guideline on Security Measures V2.0	D1 Secure ICT Procurement in Electronic Communications	D1 Security Guide for ICT Procurement; Protection of underground electronic communications infrastructure
Total views	17,017	6,574	2,594	4,733	1,625	1,491
Total EU views	7,974	2,552	1,369	2,396	752	905
Time scope of data	01.09/ 01.12.2014-31.12.2015	01.09.2014-31.12.2015	01.09.2014-31.12.2015	01.09.2014-31.12.2015	01.12.2014-31-12-2015	01.12.2014-31-12-2015

In 55.8% of the cases, the medium cannot be determined, while 28.2% were generated by organic searches, 15.8% by referral, and 0.2% through other sources such as social media. In terms of the medium used, WPK 3.2. deviates from the average (taken from all WPKs and shown in section 7.21 above) since more than a fourth of all downloads were generated by organic sources, which is exemplified by the "Technical Guideline on Incident Reporting V2.1", where

37% of downloads were facilitated by such sources. Another publication which can be described as an outlier is ”Protection of underground electronic communications infrastructure” where 0.77% of downloads were mediated by twitter (leading to six downloads in Spain and one in France), making it the most downloaded publication by way of social media amongst all deliverables covered by this study.

7.29 Work Package 3.3

In this section, download statistics for WPK 3.3´s deliverables are presented for two publications, namely:

- D2: Best practice guide on exchange processing of actionable information — exercise material
- D3: Stocktaking of standards formats used in exchange of processing actionable information

In total these deliverables were downloaded 5,386 times in the EU (out of a total 14,960 downloads of those publications world-wide). Comparatively speaking the D2 and D3 deliverables under WPK 3.3 represent 7.5 % of all ENISA downloads in the EU.

Table 37 Overview of downloads for WPK 3.3

	WPK 3.3 total	D2 Best practice guide on exchange processing of actionable information — exercise material	D3 Stocktaking of standards formats used in exchange of processing actionable information
Total views	14,960	5,145	9,815
Total EU views	5,386	2,297	3,089
Time scope of data	01.01.2015-31.12.2015	01.01.2015-31.12.2015	01.01.2015-31.12.2015

On the basis of the statistics provided, it is generally difficult to conclude on how the majority of users found the ENISA deliverables under WPK 3.3, since the statistics, on average (across the three deliverables), do not report a medium for 59.8% of the views; 16.7% of the downloads were generated by organic searchers and 23.4% by referral. For the publication “Best practice guide on exchange processing of actionable information — exercise material”, 0.09% (one download in France and Spain respectively) of the downloads were done using twitter as the medium. In terms of the EU views, the downloads of these publications stand out from the average since 36% took place within the EU (compared to the average of 46% across all deliverables and work packages). The key explanatory factor for this is that 50% of the downloads of D3 took place in China (1,147 downloads) and the United States (3,757 downloads).

APPENDIX 7
UPDATED ANALYSIS OF THE EFFICIENCY OF 2014 CORE OPERATIONAL ACTIVITIES

The KIIs set in the 2015 Work Programme were achieved by all deliverables. An overview of each work stream and the covered deliverables including targeted KIIs and achievements, as well as the publications under each deliverable, can be found in the table below.

Most deliverables include the publication of a report. Reports are available for download on the ENISA website and statistics of downloads show that, in 2014, reports were downloaded more than 125,000 times. The most downloaded reports in 2014 were "Algorithms, key size and parameters report. Study on cryptographic protocols" from 2014 (20,682) as well as "ENISA Threat Landscape" from 2014 (17,459 downloads). One of the reports with the lowest numbers of downloads was that related to the Impact assessment and roadmap (CERT).

All deliverables included as core operational activities, the number of downloads and the costs are presented in the table below.

Workstream	Workpackage	No	Deliverable title/report	Cost EUR	Downloads	Cost per download EUR
WS1 - Support EU Policy Building **Staff resources** **FTE 9.3**	WPK 1.1 Identifying evolving threats, risks and challenges	D1	ENISA Threat Landscape 2014	60024	17459	3,44
		D2	Threat Landscape and good practice guide for smart home and converged media	25000	4722	5,29
			Threat Landscape and good practice guide for Internet infrastructures	24588	5503	4,47
	WPK1.2 Contributing to EU policy initiatives	D3	Algorithms, key size and parameters report 2014/Study on cryptographic protocols	72472	20682	3,50

Workstream	Workpackage	No	Deliverable title/report	Cost EUR	Downloads	Cost per download EUR
	WPK1.3 Supporting the EU in education, research and standardisation	D1	Standardisation in the field of Electronic Identities and Trust Service Providers	30288	2374	12,76
Total WS1				**212372**	**50740**	4,19
WS2 - Support Capacity Building Staff resources FTE 12.6	WPK 2.1 Support Member States' capacity building	D2	An evaluation framework for Cyber Security Strategies	39386	14792	2,66
		D6	Impact assessment and roadmap (CERT)	80476	1397	57,61
	WPK 2.2 Support Private Sector Capacity Building	D2	Smart grid security certification in Europe;	42450	3185	13,33
		D3	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts;	48528	5042	9,62
		D5	Minimum Security Measures for Cloud Computing (two reports)	37722	11429	3,30
		D7	Methodologies for the identification of critical information infrastructure assets and services	33618	3297	10,20
		D8	Network and Information Security in the Finance Sector — Regulatory landscape and Industry priorities	49282	6371	7,74
Total WS2				**331462**	**45513**	7,28
WS3 - Support Cooperation **Staff resources** **FTE 14.0**	WPK 3.1 Crisis cooperation - exercises	D1	Cyber Europe 2014: Exercise Plan and Exercise	127944	1,400 Participants	91.39 (per participant)
			Report on Cyber Crisis Cooperation and Management	30138	2652	11,36
	WPK 3.2 Implementation of EU legislation	D1	Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents	62132	17017	3,65

Workstream	Workpackage	No	Deliverable title/report	Cost EUR	Downloads	Cost per download EUR
	WPK 3.3 Regular cooperation among NIS communities	D2	Best practice guide on exchange processing of actionable information — exercise material	93000	9815	9,48
Total WS3				**185270**	**29484**	**6,28**

APPENDIX 8
AGGREGATE DATA ON DOWNLOADS OF PUBLICATIONS - 2014 CORE OPERATIONAL ACTIVITIES

This annex is linked to the previous annex presenting an analysis of downloads of ENISA's 2015 Core Operational Activities in that it contains four tables which present the aggregated data extracted from Google Analytics. The first table looks at downloads per deliverable in total, within the EU, and the number where the location could not be determined (country not set). The second and third table present the number of downloads per publication by Member States. The forth presents the medium used to reach the downloaded publication.

Table 38 Overview of total downloads, EU downloads and other

WPK	Deliverable	Publication	Total downloads	Total EU downloads	Country Not set
WPK 1.1	D1	ENISA Threat Landscape 2014	17459	8353	196
WPK 1.1	D2	Threat Landscape and good practice guide for smart home and converged media	4722	2211	52
WPK 1.1	D2	Report: Threat Landscape of Internet Infrastructure	5503	2993	62
WPK 1.2	D3	Algorithms, key size and parameters report 2014	12344	6053	398
WPK 1.2	D3	Study on cryptographic protocols	8338	3901	227
WPK 1.3	D1	Standardisation in the field of Electronic Identities and Trust Service Providers	2374	1354	23
WPK 2.1	D2	An evaluation framework for Cyber Security Strategies	14792	3788	331
WPK 2.1	D5	CERT exercise material (all exercise material)	16159	9744	428
WPK 2.1	D6	Impact assessment and roadmap	1397	750	19
WPK 2.2	D2	Smart grid security certification in Europe	3185	2048	41
WPK 2.2	D3	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts	5042	2224	113
WPK 2.2	D5	Cloud Security Guide for SMEs	11429	4100	243
WPK 2.2	D6	Security framework for governmental clouds	7850	3693	85

WPK	Deliverable	Publication	Total downloads	Total EU downloads	Country Not set
WPK 2.2	D7	Methodologies for the identification of critical information infrastructure assets and services	3297	1946	49
WPK 2.2	D8	Network and Information Security in the Finance Sector	6371	3059	222
WPK 3.1	D2	Report on Cyber Crisis Cooperation and Management	2652	1761	47
WPK 3.2	D1	Annual Incidents report 2013	6574	2552	162
WPK 3.2	D1	Technical Guideline on Incident Reporting V2.1	2594	1369	47
WPK 3.2	D1	Technical Guideline on Security Measures V2.0	4733	2396	97
WPK 3.2	D1	Secure ICT Procurement in Electronic Communications	1625	752	102
WPK 3.2	D1	Security Guide for ICT Procurement; Protection of underground electronic communications infrastructure	1491	905	17
WPK 3.3	D2	Best practice guide on exchange processing of actionable information — exercise material	5145	2297	119
WPK 3.3	D3	Stocktaking of standards formats used in exchange of processing actionable information	9815	3089	232

Table 39 Downloads by WPK, Deliverable, publication and per Member State - Austria to Latvia

WPK	Deliverable	Publication	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Lativa
WPK 1.1	D1	ENISA Threat Landscape 2014	289	463	32	38	7	74	133	95	302	766	1288	254	42	137	774	29
WPK 1.1	D2	Threat Landscape and good practice guide for smart home and converged media	150	137	13	6	3	13	18	6	44	229	462	171	11	29	107	2
WPK 1.1	D2	Report: Threat Landscape of Internet Infrastructure	121	89	14	18	7	22	52	17	84	239	993	115	11	58	189	4
WPK 1.2	D3	Algorithms, key size and parameters report 2014	254	324	26	19	5	442	87	54	111	865	1200	106	99	72	205	14
WPK 1.2	D3	Study on cryptographic protocols	180	178	20	22	7	232	50	21	121	512	627	132	57	52	266	20
WPK 1.3	D1	Standardisation in the field of Electronic Identities and Trust Service Providers	65	85	23	12	2	63	54	16	44	213	168	47	16	11	107	3
WPK 2.1	D2	An evaluation framework for Cyber Security Strategies	119	239	38	20	5	30	35	37	96	617	551	143	40	54	248	11
WPK 2.1	D5	CERT exercise material (all exercise material)	1072	104	31	66	6	35	67	64	193	945	3972	381	20	160	309	57
WPK 2.1	D6	Impact assessment and roadmap	118	108	4	5	0	1	5	3	12	78	147	43	2	13	45	3

WPK	Deliverable	Publication	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Lativa
WPK 2.2	D2	Smart grid security certification in Europe	161	120	5	8	2	22	67	5	42	329	447	87	22	16	129	3
WPK 2.2	D3	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts	106	96	10	26	5	15	33	13	40	265	349	82	12	33	133	6
WPK 2.2	D5	Cloud Security Guide for SMEs	135	233	17	16	15	37	71	20	94	796	455	150	24	87	251	15
WPK 2.2	D6	Security framework for governmental clouds	187	152	11	15	2	39	86	35	42	184	1253	109	26	61	172	7
WPK 2.2	D7	Methodologies for the identification of critical information infrastructure assets and services	87	144	17	34	4	22	58	24	51	161	267	156	21	17	129	9
WPK 2.2	D8	Network and Information Security in the Finance Sector	115	268	13	48	9	26	57	10	55	212	340	122	17	71	191	15
WPK 3.1	D2	Report on Cyber Crisis Cooperation and Management	181	92	7	6	2	9	9	13	16	160	658	86	23	7	82	4
WPK 3.2	D1	Annual Incidents report 2013	96	140	17	11	15	22	41	18	76	243	412	156	76	23	170	10

WPK	Deliverable	Publication	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Lativa
WPK 3.2	D1	Technical Guideline on Incident Reporting V2.1	81	64	14	10	9	18	6	8	16	111	214	83	9	12	110	5
WPK 3.2	D1	Technical Guideline on Security Measures V2.0	141	114	25	12	6	16	26	17	44	183	494	94	14	11	181	13
WPK 3.2	D1	Secure ICT Procurement in Electronic Communications	53	27	7	5	1	11	8	7	23	70	147	36	2	17	37	6
WPK 3.2	D1	Security Guide for ICT Procurement; Protection of underground electronic communications infrastructure	92	35	7	6	2	7	19	8	38	80	134	54	2	16	59	4
WPK 3.3	D2	Best practice guide on exchange processing of actionable information — exercise material	118	107	18	8	2	32	20	10	27	370	271	59	7	33	133	1
WPK 3.3	D3	Stocktaking of standards formats used in exchange of processing actionable information	140	149	16	11	2	20	22	8	34	444	380	100	9	37	127	2

Table 40 Downloads by WPK, Deliverable, publication and per Member State - Lithuania to United Kingdom

WPK	Deliverable	Publication	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom

WPK	Deliverable	Publication	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
WPK 1.1	D1	ENISA Threat Landscape 2014	53	138	18	662	118	137	86	32	16	663	230	1477
WPK 1.1	D2	Threat Landscape and good practice guide for smart home and converged media	9	21	5	85	53	24	43	9	11	140	115	295
WPK 1.1	D2	Report: Threat Landscape of Internet Infrastructure	9	14	13	152	53	29	28	6	11	300	41	304
WPK 1.2	D3	Algorithms, key size and parameters report 2014	20	46	3	521	136	159	80	52	13	214	174	752
WPK 1.2	D3	Study on cryptographic protocols	8	29	3	197	90	98	65	40	12	167	71	624
WPK 1.3	D1	Standardisation in the field of Electronic Identities and Trust Service Providers	6	29	1	56	52	39	14	25	3	63	21	116
WPK 2.1	D2	An evaluation framework for Cyber Security Strategies	43	19	8	200	140	86	66	33	27	214	78	591
WPK 2.1	D5	CERT exercise material (all materials)	34	62	13	187	297	297	104	45	2	461	272	488
WPK 2.1	D6	Impact assessment and roadmap	1	3	1	39	20	7	10	4	2	17	2	57
WPK 2.2	D2	Smart grid security certification in Europe	5	13	1	109	33	34	44	6	9	131	36	162

WPK	Deliverable	Publication	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
WPK 2.2	D3	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts	11	10	3	150	64	28	65	14	12	351	48	244
WPK 2.2	D5	Cloud Security Guide for SMEs	7	47	6	249	68	60	67	15	16	267	102	780
WPK 2.2	D6	Security framework for governmental clouds	9	21	13	157	46	96	35	16	25	261	43	590
WPK 2.2	D7	Methodologies for the identification of critical information infrastructure assets and services	34	17	16	68	71	51	69	13	7	194	44	161
WPK 2.2	D8	Network and Information Security in the Finance Sector	3	44	9	165	67	65	34	8	18	211	60	806
WPK 3.1	D2	Report on Cyber Crisis Cooperation and Management	2	11	1	68	24	26	24	4	1	75	69	101
WPK 3.2	D1	Annual Incidents report 2013	22	30	8	143	58	97	65	22	15	176	62	328
WPK 3.2	D1	Technical Guideline on Incident Reporting V2.1	10	13	3	61	37	39	21	16	7	253	19	120

WPK	Deliverable	Publication	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	United Kingdom
WPK 3.2	D1	Technical Guideline on Security Measures V2.0	7	22	4	126	57	92	28	20	12	360	34	243
WPK 3.2	D1	Secure ICT Procurement in Electronic Communications	0	4	2	45	19	29	7	1	19	45	30	94
WPK 3.2	D1	Security Guide for ICT Procurement; Protection of underground electronic communications infrastructure	3	6	4	105	21	17	32	5	5	56	31	57
WPK 3.3	D2	Best practice guide on exchange processing of actionable information — exercise material	8	16	0	116	356	46	44	6	7	219	19	244
WPK 3.3	D3	Stocktaking of standards formats used in exchange of processing actionable information	6	38	0	158	689	52	31	21	9	185	43	356

Table 41 Percentage of downloads by medium used

WPK	Deliver-able	Publication	Referral (EU)	Organic (EU)	None (EU)	Other (EU)
WPK 1.1	D1	ENISA Threat Landscape 2014	13.83%	33.43%	52.70%	0.05%
WPK 1.1	D2	Threat Landscape and good practice guide for smart home and converged media	13.05%	15.76%	71.09%	0.11%
WPK 1.1	D2	Report: Threat Landscape of Internet Infrastructure	14.50%	15.05%	70.43%	0.02%
WPK 1.2	D3	Algorithms, key size and parameters report 2014	14.84%	18.72%	66.43%	0.02%
WPK 1.2	D3	Study on cryptographic protocols	16.20%	16.53%	67.26%	0.00%
WPK 1.3	D1	Standardisation in the field of Electronic Identities and Trust Service Providers	13.66%	22.23%	64.11%	0.00%
WPK 2.1	D2	An evaluation framework for Cyber Security Strategies	12.91%	32.21%	54.80%	0.08%
WPK 2.1	D5	CERT exercise material (all materials)	11.40%	11.00%	77.59%	0.01%
WPK 2.1	D6	Impact assessment and roadmap	9.33%	25.60%	64.93%	0.13%
WPK 2.2	D2	Smart grid security certification in Europe	17.33%	22.95%	59.67%	0.05%
WPK 2.2	D3	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts	19.83%	27.11%	52.97%	0.09%
WPK 2.2	D5	Cloud Security Guide for SMEs	16.49%	25.73%	57.73%	0.05%
WPK 2.2	D6	Security framework for governmental clouds	30.03%	17.22%	52.61%	0.14%

WPK	Deliver-able	Publication	Referral (EU)	Organic (EU)	None (EU)	Other (EU)
WPK 2.2	D7	Methodologies for the identification of critical information infrastructure assets and services	16.70%	35.30%	47.89%	0.10%
WPK 2.2	D8	Network and Information Security in the Finance Sector	9.97%	27.36%	62.67%	0.00%
WPK 3.1	D2	Report on Cyber Crisis Cooperation and Management	14.42%	20.90%	64.51%	0.17%
WPK 3.2	D1	Annual Incidents report 2013	17.44%	31.07%	51.49%	0.00%
WPK 3.2	D1	Technical Guideline on Incident Reporting V2.1	12.93%	36.82%	50.18%	0.07%
WPK 3.2	D1	Technical Guideline on Security Measures V2.0	17.53%	32.10%	50.33%	0.04%
WPK 3.2	D1	Secure ICT Procurement in Electronic Communications	17.55%	20.61%	61.84%	0.00%
WPK 3.2	D1	Security Guide for ICT Procurement; Protection of underground electronic communications infrastructure	13.37%	20.44%	65.41%	0.77%
WPK 3.3	D2	Best practice guide on exchange processing of actionable information — exercise material	20.03%	16.85%	63.04%	0.09%
WPK 3.3	D3	Stocktaking of standards formats used in exchange of processing actionable information	26.80%	16.64%	56.56%	0.00%

APPENDIX 9
REDESIGNED ENISA EVALUATION FORMS

In line with good monitoring and evaluation practices, ENISA asks participants to fill in evaluation forms after trainings and events. In order to ensure that these forms focus more on outcomes relative to organisational aspects, we have redesigned them and developed an additional follow-up form. Depending on the form these take, their final content and their implementation, their results could be fed into next year's evaluation. The redesign draws both on our general experience designing such forms, as well as our specific experience collecting data to evaluate and assess ENISA´s activities. Overall, the redesign has been based on the following principles:

- **Continuity:** Ensuring that the original content of the forms is still included to make comparison over years possible, and since ENISA staff may be relying on this information in their work.

- **Inference:** Ensuring that the forms allow ENISA and the evaluator to use the data derived to assess the effectiveness of events and improve them.

- **Validity:** Ensuring that the data derived from the evaluation forms accurately reflects the views of the respondent.

The following forms have been redesigned and can be found below:

1. Evaluation form for training sessions and events
2. Evaluation survey Strategic Level Exercises (SLEx)
3. Evaluation survey for Technical Level Exercises (TLEx)

In addition to these, we have developed two new evaluation forms, and these can also be found below:

4. Brief survey of users when they download forms from ENISA´s website
5. A flexible follow-up form to be submitted 3 months after trainings and events (including the SLEx and TLEx) have been completed

Importantly, the evaluation form for trainings has been redesigned using the same format as the previous form. This means that the form is still envisaged to be distributed on paper (one A4 page printed on both sides). While this has certain advantages, in particular since it makes it easy to distribute the form once the event/training has been completed, it entails administrative costs and will not allow for a comparison with the proposed follow-up form. The evaluation form could be implemented via an online survey distributed to participants via their email-addresses immediately after a training session or event ends. If participants have their laptops, smartphones or tablets at hand, the survey could be sent directly by the organiser to participants in the last five minutes of the event, and participants could be encouraged to immediately answer the survey. The advantages of this would include:

- Responses from participants can easily be extracted to excel for further analysis, without having to enter the information on the paper forms into the survey software, which would save staff time.
- Responses from participants could be linked to their email addresses, meaning that the information given in the evaluation form could be compared to information provided in the follow-up form. This would allow ENISA to examine whether participants' immediate assessment of the training session/event changed once they have had a chance to apply its lessons over the period of three months after the end of the training session/event.

Depending on the implementation of the survey, anonymity or confidentially of the respondents can still be maintained.

If both the evaluation form and the follow-up form are filled in online and respondents can be identified (either via email address or an anonymous respondent code), then we propose further developing the redesigned evaluation form to be suitable for an online survey format. In addition, we recommend adding two additional questions to the evaluation form, which would allow ENISA to more closely examine the usefulness and impact of the Agency´s trainings and events (these are highlighted in blue font in the redesigned forms).

1. Evaluation form for training sessions and events

The evaluation form is intended to be distributed immediately after an event or training session finishes. The layout of ENISA´s current form has been kept the same, and all the original questions are still included. New questions are included in either **green** or **blue**: The green questions should be included regardless of whether the form is completed on paper (as currently) or online. The blue questions should be included if the form is implemented online and if the follow-up survey is also implemented.

1- Name, and country (optional):

2- Email *(to be included if this evaluation is conducted online. It will allow for a comparison of responses over time):*

3- How do you rate the training session?

	5	4	3	2	1
Overall impression					
Trainers					
Training session ("Mobile Threats and Incident handling")					
Training session ("Memory forensics")					
Training session ("Artefact Analysis")					
I would like to participate in other workshops the following years					

(5=liked very much, 1=did not

like)

4- By taking part in this [INSERT event type], I expected to (multiple options are possible):

- Develop a concrete output (e.g. guideline, recommendation, best working practice/administrative procedure)
- Gain further knowledge
- Develop new skills
- Identify and share best practices
- Extend my network of contacts across Europe
- Contribute to (new) network and information security policies, standards and/or procedures
- Other, please specify:

5 - To what extent were your expectations met? Please provide a rating below:
- Fully
- Mostly
- Only partially
- Not at all
- Don’t know

6- Provide further details below of why your expectations were only partially or not at all met:

Please turn the page to complete the last two questions

7 - To what extent was the training session useful to your work? Please provide a rating below

□ Very useful to my work

□ Useful to my work

□ Not very useful to my work

□ Not at all useful to my work

□ I do not know

8 - What do you intend to do with what you learnt / developed?

□ Forward the output (e.g. guideline, report etc.) of the activity to colleague(s)

□ Draft a summary/report to send to colleagues

□ Draft a summary/report which was published on our intranet

□ Talk with colleagues about my experiences

□ Talk with my superior about my experiences

□ Organise a meeting to share my experiences

□ Help organise an internal training session / workshop on what I had learned

The place of venue/catering

9-This is my opinion about the place of venue and the catering:

Didn't like

Liked very much

□ □ □ □

□

The future

Further comments

(Here's room for anything else you want to tell us)

YOUR COMMENTS ARE VERY MUCH APPRECIATED. PLEASE HAND THIS EVALUATION FORM TO A MEMBER OF THE WORKSHOP STAFF OR LEAVE IT ON YOUR TABLE FOR COLLECTION.

Thank you for your time!

ENISA

2. Cyber Europe 2014 – Strategic Level Exercise – Evaluation Survey

This is the SLex evaluation survey used in 2014. This evaluation survey is intended to be distributed shortly after an event or training finishes. The layout of ENISA´s current form has been kept the same, and all the original questions are still included. New questions are included in either **green** or **blue**: The green questions should be included regardless of whether the form the form is followed by our proposed follow-up form, while the blue questions should only be included if the follow-up survey is also implemented.

Remark: no formatting as the questionnaire should be CEP-based

(1-5) questions should include a small box for people to provide further justification if needed

Exercise planning

- Was the list of questions in the ExPlan helpful?
- Was it easy to recruit players for the exercise? (1-5)
- Was the state of the world (SOW) material helpful to brief your players prior to the exercise? (1-5)
- Please provide any other comment that would have helped to improve **the planning** SLEx? (free text)

Exercise conduct

- To what extent did you find the conduct of SLEx as a moderated tabletop, with two moderators driving the discussions forward, appropriate to achieve the objectives of the exercise? (1-5)
- To what extend did you find the presentations of day 1 useful? (1-5)
- To what extent do you think that the actual participants to the Strategic Level Exercise were the right ones? (1-5)
- Please provide any other comment that would have helped to improve **the conduct** of SLEx? (free text)

Exercise outcomes

- To what extent do you feel your players learned from the two-day event? (1-5)
- How satisfactory was the event to them? (1-5)
- To what extent would you say this first Strategic Level Exercise will reflect on the way in which national cyber crisis management is handled (notably with regards to the international dimension)?
- According to your assessment what is(are) the main outcome(s) of two days event? (free text)

Logistics

- How did you find overall the organisation logistics of the workshop (ENISA, Commission, catering, giveaways, etc.)? (1-5)
- To what extent would you argue that the social event, and notably the cooperation puzzle, participated to breaking the ice between the participants? (1-5)
- Was the split of the Workshop in two-half days good for you and your players? (1-5)
- Please provide any other comment that would have helped to improve **the logistics** of SLEx? (free text)

Exercise usefulness

- To what extent was the training session useful to your work? Please provide a rating below

□ Very useful to my work
□ Useful to my work
□ Not very useful to my work
□ Not at all useful to my work
□ I do not know

- What do you intend to do with what you leant / developed?
  - □ Forward any written material (output) (e.g. course material or presentations) to colleague(s)
  - □ Draft a summary/report to send to colleagues (e.g. concerning lesson learned)
  - □ Draft a summary/report which was published on our intranet (e.g. concerning lesson learned)
  - □ Talk with colleagues about my experiences (e.g. lesson learned)
  - □ Talk with my superior about my experiences (e.g. lesson learned)
  - □ Organise a meeting to share my experiences (e.g. lesson learned)
  - □ Help organise an internal training session / workshop on what I had learned

3. TLEx Evaluation form

This form (originally titled TLEx Evaluation questions) is intended to be distributed shortly after an event or training finishes. The layout of ENISA´s current form has been kept the same (although the front page and last page has been removed), and all the original questions are still included. New questions are included in either **green** or **blue**: The green questions should be included regardless of whether the form the form is followed by our proposed follow-up form, while the blue questions should only be included if the follow-up survey is also implemented.

GENERAL INFORMATION	
Organization/Company/Team Name:	
Country:	
Sector:	
Additional Information (ex. No of people in Team, Injects Solved):	
Contact Information (email):	

Exercise usefulness

1- To what extent was the exercise useful to your work? Please provide a rating below

□ Very useful to my work

□ Useful to my work

□ Not very useful to my work

□ Not at all useful to my work

□ I do not know

2- What do you intend to do with what you leant / developed?

□ Forward any written material (output) (e.g. course material or presentations) to colleague(s)

□ Draft a summary/report to send to colleagues (e.g. concerning lessons learned)

- □ Draft a summary/report which was published on our intranet (e.g. concerning lessons learned)
- □ Talk with colleagues about my experiences (e.g. lesson learned)
- □ Talk with my superior about my experiences (e.g. lesson learned)
- □ Organise a meeting to share my experiences (e.g. lesson learned)
- □ Help organise an internal training session / workshop on what I had learned

The criteria listed below will help you evaluate the CE2014 TLEx experience. Please discuss the questions with your TLEx team in order to capture the overall opinion as far the technical and operational aspects of the exercise are concerned. Scoring is based on a scale from 1 to 5. 1 means that the exercise aspect didn't fit your technical teams criteria, and 5 means that the exercise aspect was satisfying.

	Evaluation Aspect	Score 1-2-3-4-5	Comments
1	Overall how do you evaluate the CE 2014 TLEx experience?		
2	Overall how do you evaluate the level difficulty of the TLEx?		
3	Overall how do you evaluate the technical skills gained by participating in the TLEX?		
4	Overall how do you evaluate the technical incidents simulated in TLEx?		
5	Overall how do you evaluate the available time given in order to solve the separate Injects?		
6	Overall how do you evaluate the pre- exercise and supporting material and information (Information package, descriptions, etc)?		
7	Overall how do you evaluate your own team's technical capabilities on solving incidents similar to TLEx?		
8	Overall how do you evaluate the use of the Cyber Exercise Platform?		
9	Overall how do you evaluate the fairness of quiz-assessment scheme used at the end of each incident?		

10	Did you value participating in CE 2014 TLEx as a player/moderator? Please evaluate.		
11	Will you be interested in participating in future Technical-level Cybersecurity Exercises?		YES/NO/Maybe
12	Would you like the future Cyber Europe exercises to continue having Technical-level incidents to be resolved?		YES/NO/Maybe
13	How long do you think future Technical-level cyber security exercises should last?		
14	Do you want future technical cyber security exercises to also have real-time capture the flag games, in addition to forensics-style cyber incident analysis?		YES/NO/Maybe
15	Do you have any other suggestions for improving the future Cyber Europe TLEx? Comment.		

For each Incident of CE 2014 TLEx please evaluate the following aspects. Scoring is based on a scale from 1 to 5. 1 means that the Inject aspect didn't fit your technical teams criteria, and 5 means that the exercise aspect was very satisfying.

Incident Number	How realistic was that incident?	Overall level of difficulty?	Quality of accompanying material (exercise files, descriptions etc.)?	Difficulty of evaluation questions?	Specify your level of interest on this specific type of incidents.
1.1					
1.2a					
1.2b					
1.2c					
2.1					
2.2					
2.3a					
2.3b					
3.1					
3.2					
4.1					
4.2					
4.3					

4. Follow-up survey

This form has been developed to gather further data on the effectiveness of ENISA´s events and trainings by following up with participants three months after the event/training ended. It is compatible with the three evaluation forms (shown above), and will allow for firmer data on the actual usefulness (relevance), dissemination, results and effects of ENISA´s events/training sessions. As explained above, this form should be implemented in extension of the existing, but redesigned forms, in order to reap those benefits. It should be implemented online by using respondents email addresses (from participants´ lists).

Introduction: *Three months ago, you participated in [INSERT name of event/training session] which was organised by ENISA. Please complete this short survey (maximum 8 questions) to share your views on the training.*

Please note that this survey is not the same as the evaluation form which you filled in after the event/training.

Usefulness

1-Three months on, I feel that from a professional point of view, the ENISA event / training session was... (Please tick the relevant box to finish the sentence)

□ Very useful

□ Useful

□ Not very useful

□ Not at all useful

□ I do not know

2- Please provide further details below of why you are of this opinion:

Dissemination

3 -Further to your participation in this ENISA event / training session, did you share what you learned with colleagues?

□ Yes (Go to Q4)
□ No (Go to Q5)

4 -How did you share what you learned (Multiple choices possible)

□ I forwarded the output (e.g. guideline, report etc.) of the activity to colleague(s)
□ I drafted a summary/report which was sent to colleagues
□ I drafted a summary/report which was published on our intranet
□ I talked with colleagues about my experiences
□ I talked with my superior about my experiences
□ I organised a meeting to share my experiences
□ I helped organise an internal training session / workshop on what I had learned
□ I shared my experiences otherwise, namely…. *[text box]*

Results

5- Have you and/or others in your organisation taken any specific actions based on the results of this ENISA event/training session?

	Yes	**No**	**Do not know**	**Not applicable**
Issued a recommendation / guideline				
Organised an internal training session				
Amended practices/ administrative procedures (e.g. SOPs or other)				
Updated or started a procedure to update network and information systems				
Other				

	Yes	**No**	**Do not know**	**Not applicable**
If other, please specify:	*[text box]*			

6-If you answered 'No' to any of the above, explain why no specific actions have been taken based on the results of the ENISA event/training session [text box]

Effects

7-Has an output of this ENISA event/training session (e.g. handbook, best practice, report, guideline etc.) led to any of the following for you and/or for your organisation? (Please respond in relation to the statements below.)

	Yes	**No**	**Do not know**
Increased knowledge			
Improved working practices/administrative procedures (e.g. SOPs…)			
Improved tools			
Other, please specify:	*[text box]*		

Networking

8-Do you think that the ENISA event/training session that you participated in provided a good opportunity for you
to expand your network of contacts abroad?

□ Yes
□ No

9-How often have you been in contact for work purposes with the officials, industry representatives, experts or other persons you met during this event /training session over the past three months?

□ Several times per month

- □ Once a month
- □ A few times (3 to 5)
- □ A couple of times (2)
- □ Once
- □ Never

Further comments

10- Please add anything else you want to tell us

YOUR COMMENTS ARE VERY MUCH APPRECIATED. PLEASE CLICK “SUBMIT” TO SEND US YOUR FEEDBACK.

Thank you for your time!
ENISA

5. Survey linked to the download of ENISA's deliverables

This survey is intended to be launched on ENISA´s website, and to pop-up when users download an ENISA publication. The purpose is to gather improved information on users of ENISA publications. In addition to the questions listed below, ENISA could consider adding a question on the country in which the users works. While this information is included in the data extracted from Google Analytics, such a question would enable ENISA to know the location of the respondent to the survey.

Introduction: *Please take 2 minutes to help ENISA improve our publications.*

6. Where did you first hear about the output/publication you just downloaded?

ENISA's website
An ENISA-organised event
An external event
A colleague
Search engine
Other *[text box]*

7. What use do you intend to make of the output/publication you just downloaded (multiple options possible)?

Read it
Reference it in my written work
Put in practice its recommendations / good practices
Further disseminate it to colleagues
Other, please describe *[text box]*

8. If you have **read/used ENISA publications before,** please rate the extent to which you agree or disagree with the following statements concerning ENISA´s publications in general:

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess
A. ENISA´s publications provide stakeholders with high quality advice and assistance						
B. ENISA´s publications help develop Member States´ and the EU´s ability to prevent, detect, analyse and respond to threats						
C. ENISA´s publications support the development and implementation of EU regulation in the area of data protection and privacy						

9. Please rate the extent to which you agree or disagree with the following statement concerning the publication you have downloaded:

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don’t know/ Cannot assess
A. I have found publications with similar content from other sources						

10. If you indicated that you have found publications with similar content, could you provide us with the source (for example, the organisation, website or institution behind the publication)? *[text box]*

11. Which of the description below fits your workplace best?

Industry (for example, digital services, financial services, electronic communication or trust services)
National or government authority (for example, ministry, agency, authority or local/regional government)
International organisation
European Institution (for example, the European Commission, the European Parliament, or European Agencies)
Academic institution
ENISA
NGO/Think tank
Other *[text box]*

Thank you for your participation.

APPENDIX 10
INTERVIEW GUIDE 2015[122]

Interviewee	
Organisation	
Date	
Interviewer	

The interviewer will begin by introducing the evaluation, its objectives and scope. Not all questions needs to be probed, but the different themes (evaluation criteria) should be explored.
Explain that the interview will start with discussing the deliverables and achievements, and then some more general questions on how the Agency functions.

Introductory questions

- What is your main area of work, can you briefly describe your main responsibilities?
- How long have you been working in this area?
- Please describe what activities during 2015 which you have been aware of/participated in.

Stakeholder	Evaluation Question	Interview questions
	Effectiveness	

[122] New elements relative to last year's interview guide are written in blue font to make them easily identifiable.

Stakeholder	Evaluation Question	Interview questions
Management Board, Commission and MEPs	**12. To what extent does ENISA achieve its objectives, as stipulated in the legal mandate?**	See the M&E Framework for relevant questions to respondents – go through indicators on results and impact for deliverables in question.
Management Board	**13. To what extent is ENISA's organisation conducive to supporting the achievement of its objectives?**	Is the current set-up of the organisation fit for purpose, in terms of the division of tasks and responsibilities? Are there areas for improvement, if so what?
Management Board	**14. To what extent are ENISA's systems and procedures conducive to supporting the achievement of its objectives?**	In your opinion, how are ENISA´s systems and procedures contributing to capacity building in the EU, enhancing cooperation etc.? What more could be done to this end? Can you please describe how you have experienced this?
All	**15. To what extent does ENISA help develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)?**	How would you describe ENISA´s contribution to maintaining a high level of expertise amongst EU actors? Does ENISA also help develop this expertise? Could you provide an example?
	16. To what extent does ENISA assist the Member States and the Commission in enhancing capacity building throughout the EU?	How would you describe ENISA´s ability to assist the Member States/the Commission in enhancing capacity building throughout the EU? Can you please describe how you have experienced this?
	17. To what extent does ENISA assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security?	How would you describe ENISA´s ability to assist the Member States/the Commission in in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security? Can you please describe how you have experienced this?
	18. To enhance cooperation both between the Member States of the EU and between related NIS?	How would you describe ENISA´s contribution to enhance cooperation both between the Member States of the EU and between related NIS? Could you provide an example of this?
	Impact	

Stakeholder	Evaluation Question	Interview questions
All	**19. To what extent do ENISA's core operational activities contribute to achieving more long term objectives (impact)?**	In your view, does ENISA contribute to ensuring a high level of NIS within the EU? What more could be done to this end, and by whom?
		In your view, does ENISA contribute to raising awareness on NIS? What more could be done to this end, and by whom?
		In your view, does ENISA contribute to promoting a culture of NIS in society? What more could be done to this end, and by whom?
	Efficiency	
Management board	To what extent does ENISA have cost saving measures in place?	Can you please describe how you overall assess the efficiency of ENISA? Do you compare costs of different activities, or conduct any other kind of analysis of costs? Do you have any specific cost saving measures in place?
	Coordination and coherence	
All	**20. To what extent does ENISA coordinate activities with relevant bodies, offices and agencies in the field of Information and Communications Technologies (ICT)?**	In your opinion, are all the relevant stakeholders that should be involved in ENISA's work covered? Are some missing? How is your organisation/institution involved? Are certain stakeholders more/less involved than others, and what are the consequences for ENISA's work and achievements?
All	**21. To what extent do ENISA's activities contradict or complement those of other public interventions?**	Are there other public bodies doing similar work to that of ENISA? In what way does ENISA's work overlap or complement their work? In your opinion, are there any adverse effects from ENISA's work? Has it happened that unintended effects occurred? If so what, please describe?

Stakeholder	Evaluation Question	Interview questions
	EU Added value	
All	**22. To what extent does ENISA contribute with relevant and reliable information, which other sources do not provide?**[123]	Apart from ENISA, which other sources of information/expertise do you use for NIS? From your perspective, does ENISA differ from other sources of information?
	23. Does the Agency (1) support national actions in general ('mirroring') or specific areas of national policy ('boosting')?	In your opinion, how does ENISA support national actions? Can you think of any cases where ENISA activities have been coordinated with other initiatives?
	24. **Are there any cases where ENISA activities are coordinated or overlap (duplication of efforts) with other bilateral or European initiatives?**	Can you think of any cases where ENISA activities have overlapped with other initiatives?

Concluding questions

- What are your expectations in relation to this evaluation?
- Do you have anything else that you would like to add?

[123] This is a new evaluation question which has been added for the evaluation of ENISA in 2015.

APPENDIX 11
SURVEY QUESTIONNAIRE

ENISA –SURVEY

Introduction to the survey

According to Financial Regulation applicable to the European Union Agency for Network and Information Security (ENISA), an ex –post evaluations shall be undertaken. Such evaluations are foreseen for all programmes and activities which entail significant spending.

Responsibility for carrying out yearly evaluations of ENISA's activities has been awarded to the company Ramboll Management Consulting (Ramboll), under a contract concluded with ENISA. The task of the evaluators is to collect information from ENISA and its stakeholders on a yearly basis, in order to assess the extent to which ENISA has been successful in reaching the objectives specified the mandate.

To this end, the evaluation team is gathering views and opinions from key stakeholders regarding the work of the Agency, by means of an electronic survey. Your contact details have been provided to the evaluation team by ENISA. Please click here < insert link > to read the information note on the evaluation.

It will take around 20 minutes to answer the survey. Once you begin, the answers are saved automatically and you can always complete the survey at a later stage by clicking on the same link. At the end of the questionnaire, you may print or save a local copy of your answers if you wish.

Your answers will be of great importance to the evaluation, and will feed into recommendations aimed at the improvement of ENISA's work.

To access the survey, please click on the following link: < insert link >

If you have questions about the evaluation, please contact Vanessa Ludden on email: VANL@ramboll.com
If you have questions of technical nature, please contact Ida Maegaard Nielsen on email: IMN@ramboll.com

Thank you for your participation.

BACKGROUND QUESTIONS

Role/Entity[124] *(Please tick all that apply)*

- *Permanent Stakeholder Group*
    - *Industry*
    - *Academia*
    - *Consumer organisation*
    - *Other, please explain ___________*
- *European Parliament*
- *European Commission*
- *National Liaison Officer*
- *Management Board*
- *Industry*[125]*:*
    - *Finance, including banking*
    - *Electronic communications, including the provision of either network or service or both*
    - *Digital service (Annex III of the adoption pending NIS directive)*
    - *Trust service (Regulation (EU) No 910/2014)*
    - *Energy*
    - *Transport*
    - *Health*
    - *Other, please describe ___________________________*
- *Other, please specify ___________________________*

Country
[Drop-down list]

RELEVANCE

[124] Interviewees will be allowed to tick multiple boxes, since some of them fulfil more than one role.

[125] This category could be further broken down with the help of ENISA if judged relevant.

25. Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to EU Policy in National Information Security (NIS):

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess
A. The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the Member States						
B. The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the EU						
C. The outputs produced by ENISA are responding to the needs for NIS in the Member States						
D. The outputs produced by ENISA are responding to the needs for NIS in the EU						

26. Please rate the extent to which you agree or disagree with the following statements concerning ENISA's ability to meet expectations

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess
A. ENISA is effectively meeting stakeholder expectations						
B. It is clear what ENISA expects from stakeholders						

27. Please provide additional comments as relevant:____

EFFECTIVENESS – SUPPORT TO EU POLICY BUILDING

28. Are you familiar with ENISA's work on developing and maintaining a high level of expertise related to NIS, facilitating voluntary information, establishing mutual interactions, and/or contributing to EU policy initiatives and supporting EU in education research and standardisation?

Yes □ No □ – jump to 31

29. Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to EU Policy in NIS:

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess
A. ENISA's deliverables about NIS threats in the EU are relevant and of high quality						
B. ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions						
C. The input provided by ENISA to *develop* new policies for NIS in the EU is useful						
D. The input provided by ENISA to *implement* new policies for NIS in the EU is useful						
E. ENISA provides stakeholders with relevant information on 9standardization, innovation and research						
F. ENISA's outputs and deliverables contribute to putting in place more effective risk mitigation strategies						
G. ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services						
H. ENISA's outputs and deliverables contribute to setting standards for NIS and privacy						
I. ENISA promotes relevant methods towards emerging technologies						

J. ENISA's activities enable opportunities for new technologies and approaches						

30. Please provide additional comments as relevant:-
____

EFFECTIVENESS – CAPACITY BUILDING

31. Are you familiar with ENISA's work to support the capacity building of EU Member States and public and private sectors, as well as its efforts to contribute to raising the level of awareness of EU citizens?

Yes □ No □ – jump to 34

32. Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to capacity building:

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess
A. Good practices in NIS have been disseminated by ENISA						
B. ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States						
C. ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or incidents						
D. The support provided by ENISA in capacity building complements that of other public interventions						
E. ENISA's support has enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis						

F. Sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA						
G. Cyber security challenges are adequately addressed in the EU and Member States						
H. Cyber security challenges are adequately addressed in the Member States						
I. ENISA's activities ensure adherence to EU Data Protection Legislation						

33. Please provide additional comments as relevant:____

EFFECTIVENESS – SUPPORTING COOPERATION

34. Are you familiar with ENISA's work to support cooperation between all stakeholders relevant and active in the area of NIS?

Yes □ No □ – jump to 37

35. Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to cooperation:

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess
A. ENISA effectively supports the sharing of information, ideas and common areas of interest among stakeholders						
B. ENISA's support to cooperation between stakeholders						

complement those of other public interventions						
C. ENISA effectively shares lessons learned from exercises with other communities and sectors						
D. ENISA's support has contributed to enhanced cooperation in operational communities						
E. ENISA's support has improved services, workflow and communication among stakeholders to respond to crises						
F. Technical capacity has increased among involved stakeholders						
G. ENISA's support has enabled emergency mitigation and responses to be put in place at low resource and time costs						
H. The support from ENISA has contributed to enhancing community building in Europe and beyond						
I. ENISA supports the development and implementation of Data Protection and Privacy regulation						
J. ENISA's increases coherence between EU funded R&D projects and the objectives of NIS policy						

36. Please provide additional comments as relevant:____

IMPACT

37. Please rate the extent to which you agree or disagree with the following statements concerning ENISA's contribution to its overall objectives:

	Strongly	Disagree	Neither	Agree	Strongly	Don't

	disagree		agree or disagree		Agree	know/ Cannot assess
A. ENISA clearly contributes to ensuring a high level of NIS within the EU						
B. ENISA clearly contributes to raising awareness on NIS within the EU						
C. ENISA clearly contributes to promoting a culture of NIS in society						

38. Please provide additional comments as relevant:____

EU ADDED VALUE[126]

39. Please rate the extent to which you agree or disagree with the following statements concerning ENISA:

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess
B. ENISA contributes with relevant and reliable information, which other sources do not provide						
C. ENISA supports national actions in general						
D. ENISA supports specific areas of national actions						
E. There are cases where ENISA activities duplicate efforts, because other similar initiatives are taking place.						

[126] This question is a new addition to the survey for the evaluation of ENISA´s activities in 2015.

40. Please provide additional comments as relevant:____

ADD-ON TO THE GENERAL SURVEY: BRIEF, TARGETED SURVEY

41. Have you made use of any ENISA publications which were published in 2015[127] or the workshop listed below? You will not be asked specific questions in relation to the publications or the workshop.

No, I have not made use of any ENISA reports, analysis or handbooks from 2015 or participated in the workshop OR

	Yes	No	Don't know/ Cannot assess
A. "Stocktaking, Analysis and Recommendations on the Protection of CIIs"[128]			
B. "CIIP Governance in the European Union Member States"[129]			
C. "Methodology for the identification of Critical Communication Networks, Links, and Components"[130]			
D. "Secure Use of Cloud Computing in the Finance Sector. Good practices and recommendations"[131]			
E. "Security and Resilience in eHealth. Security Challenges and Risks"[132]			
F. "Mobile Threats Incident Handling. Handbook, Document for teachers"			

[127] Some publications were published in early 2016, but where developed under the Agency´s 2015 work programme.

[128] Published December 2015

[129] Please note that there is restricted access to this report.

[130] Published October 2015

[131] Published December 2015

[132] Published December 2015

G. "Introduction to advanced artefact analysis. Handbook, Document for teachers"			
H. "Advanced dynamic analysis. Handbook, Document For Teachers"			
I. "Advanced static analysis. Handbook, Document for teachers"			
J. "Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations"			
K. "Leading the way. ENISA's CSIRT-related capacity building activities. Impact Analysis – Update 2015"			
L. "Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. Methodology, Pilot Assessment, and Continuity Plan"			
M. "Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics"			
N. Participated in the **workshop** "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA event"			

42. Please provide additional comments as relevant:____

If the respondent answers yes to any of the questions above jump to question 19[133], otherwise the survey ends.

43. Please rate the extent to which you agree or disagree with the following statements concerning ENISA:

	Strongly disagree	Disagree	Neither agree or disagree	Agree	Strongly Agree	Don't know/ Cannot assess

[133] The responses to question 19 can be cross-tabulated with the specific publications/workshop shown under question 17. This means that we can identify respondents who state that they have used a given publications and their agreement with the statements on outcomes below, thus linking usage to a given outcome in the analysis.

D. ENISA´s work, outputs and publications provide stakeholders of CII with advice and assistance						
E. ENISA´s work, outputs and publications help develop Member States´ and the EU´s ability to prevent, detect, analyse and respond to threats						
F. ENISA´s work, outputs and publications have supported the development and implementation of EU regulation in the area of data protection and privacy						
G. ENISA´s workshop "Cyber Security Strategies, Critical Information Infrastructures Protection and ICS SCADA event" has helped disseminate good practices regarding cyber security among private and public stakeholders.						

44. Please provide additional comments as relevant:____

45. Would you be available to take part in a short interview regarding your experience with ENISA´s activities? The duration and timing of the interview will be decided based on your availability.

    Please provide your email address, so that we can contact you to look into the possibility of setting up an interview:___________________________

46. Do you have any particular suggestions as to how ENISA could improve in the future? ____

THE SURVEY IS NOW FINALISED. MANY THANKS FOR YOUR PARTICIPATION!

[Text]