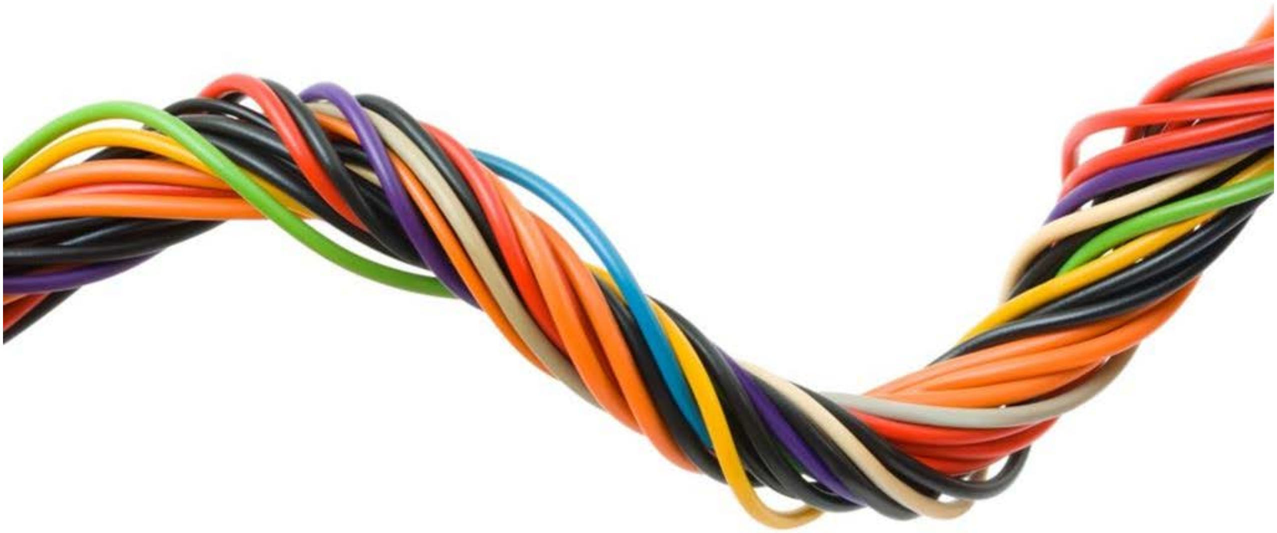
Intended for
ENISA

Document type
Final report

Date
September 2015

Framework contract No F-DIR-15-C12

EXTERNAL EVALUATION OF ENISA
FINAL REPORT



EXTERNAL EVALUATION OF ENISA
FINAL REPORT

Revision	**Final**
Date	**07/10/2015**
Made by	**KARA/VANL/FRAN**
Checked by	**HELU**
Approved by	**HELU**
Description	**Final report**

Ramboll
Hannemanns Allé 53
DK-2300 Copenhagen S
Denmark
T +45 5161 1000
F +45 5161 1001
www.ramboll.com

CONTENTS

1. INTRODUCTION 1

2. POLICY CONTEXT IN THE AREA OF NETWORK AND INFORMATION SECURITY 2

2.1 EU´s role in developing Network and Information Security and establishment of ENISA 2

2.2 Legal background and mission 4

2.2.1 ENISA's objectives 4

2.3 The Agency's tasks and activities 5

2.4 ENISA's stakeholders 5

3. METHODOLOGY OF THE EVALUATION 7

3.1 Sources and data collection 8

4. DESCRIPTION OF ENISA'S ORGANISATION 9

4.1 The organisation of the Agency 9

4.2 Management systems and procedures 12

4.3 Collaboration and communication 12

5. FINDINGS OF THE EVALUATION 13

5.1 Overall relevance of ENISA's activities 13

5.2 Overall impact of ENISA's activities 16

5.3 Effectiveness of ENISA's activities: Evaluation findings related to 2014 Work Streams 17

5.3.1 Achievement of Key Impact Indicators (KII) and statistics on downloads 17

5.3.2 Work stream 1: Support EU policy building 18

5.3.3 Work stream 2: Support capacity building 20

5.3.4 Work stream 3: Support co-operation 23

5.4 Efficiency 26

5.4.1 Costs and resources per work stream 26

5.5 Coordination and coherence 29

6. CONCLUSIONS AND RECOMMENDATIONS 30

6.1 Relevance 30

6.2 Effectiveness 30

6.3 Efficiency 31

6.4 Coordination and coherence 31

7. ACTION PLAN 32

FIGURES

Figure 1 Timeline of key developments in NIS in Europe 3
Figure 2. Specific objectives of ENISA... 4
Figure 3. ENISA's stakeholder map 6
Figure 4: Our approach to the evaluation of ENISA's core operational activities 7
Figure 4: ENISA organisational chart 10
Figure 5 ENISA's budget 2011-2015...11
Figure 6 Q3.8 Cyber security challenges are adequately addressed in the EU 14
Figure 7 Q1.2 The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the EU...14
Figure 8 Q1.7 It is clear what ENISA expects from stakeholders 15
Figure 9 Q2.2 ENISA's deliverables about NIS threats in the EU are relevant and of high quality 18
Figure 10 Q2.8 ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services...19
Figure 12 ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States 21
Figure 12 Q3.4 ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or incidents 22
Figure 13 Q3.7 Sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA 22
Figure 14 Q4.6 ENISA's support has improved services, workflow and communication among stakeholders to respond to crises 23
Figure 16 Q4.4 ENISA effectively shares lessons learned from cyber exercises with other communities and sectors 24
Figure 16 Q4.5 ENISA's support has contributed to enhanced cooperation in operational communities...25
Figure 17 Q3.3 The support provided by ENISA in capacity building complements that of other public interventions..29

TABLES

Table 1 Data collection and sources.. 8
Table 2 Response rates survey to stakeholders... 8
Table 3 Staff by category end of year 11
Table 4 Overview cost and staff per deliverable (source ENISA) 28

ANNEXES

Annex A Survey results
Annex B Evaluation matrices and score board
Annex C Core Operational Activities 2014
Annex D Case study report CE2014

Abbreviations

CE2014	Cyber Europe 2014
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
COA	Core Operational Activities
COD	Core Operations Department
D1	Deliverable 1
DAE	Digital Agenda for Europe
EC	European Commission
EFTA	European Free Trade Association
ENISA	European Union Agency for Network and Information Security
EU	European Union
e-IDs	Electronic Identifications
FTE	Full-time employee
KIIs	Key Impact Indicators
MB	Management Board
MFF	Multiannual Financial Framework
NIS	Network Information Security
NLO	National Liaison Officers
OECD	Organisation for Economically Developed Countries
PSG	Private Stakeholder Group
QMS	Quality Management System

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

EXECUTIVE SUMMARY

This report presents the findings and conclusions from the **external evaluation of ENISA's core operational activities in 2014**. 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 scope of the evaluation focussed on ENISA's **core operational activities** in 2014, with an **estimated expenditure above 30,000** Euros. Data has been collected among **key stakeholders** (public and private) through an on-line survey. Group interviews were conducted with **operational staff at ENISA** in Athens and phone interviews were undertaken with players and moderators in the **CE2014 exercise** (as a case study). All in all, while the data collected is considered of good quality, the **limited number of respondents** reached makes it difficult to establish the validity and reliability of information provided; this will need to be addressed in subsequent evaluations.

Overall, the evaluation findings are positive and on most indicators ENISA's Work Programme 2014 has **achieved the intended outcomes, results and impacts**, as per the judgment norm agreed for the evaluation. There is a clear pattern in terms of progress, **where targets under ENISA's control (such a high quality, community building, good practice dissemination) are largely achieved**. The progress towards **more long term objectives looks more uncertain (preparedness to respond to crises, increase in capacity etc.)**, as this is **highly dependent on contextual factor**s as well as public and private stakeholders' engagement and investment.

The **scope and objectives of ENISA's work is seen as relevant** to respond to the needs, but at the same time **stakeholders see limits in ENISA's mandate and outreach**. In particular, private stakeholders and industry appear to strive towards a more operational role for ENISA, going beyond the advisory and facilitating mandate of the Agency, in order to effectively achieve the overall objectives of Network Information Security (NIS) and cyber security.

The **operational budget of ENISA is limited**, and the main expenditure relates to staff costs. 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. No indication of low efficiency was identified in the evaluation period, though specific cost saving measures could not be established.

Overall, it can be concluded that **ENISA effectively cooperates and engages** with its main stakeholders, as stipulated in its mandate. The support provided by ENISA is seen as a complement to that of other public interventions, and **no adverse effects were identified**.

ENISA's appears to **fulfil its mandate and achieve the set objectives**. Hence, there is **no call for immediate or urgent actions** to be taken on the basis of the evaluation. However, to further increase effectiveness and relevance, it is suggested that ENISA continue to explore ways to ensure ENISA's work is **addressing real needs in NIS in the EU**. Given the limited resources available to the Agency, it may be important in the future **to focus on activities where there is a strong demand** from the NIS communities to **ensure that ENISA's deliverables achieve a real impact**.

1. INTRODUCTION

This final report presents the findings and conclusions from the external evaluation of ENISA's core operational activities in 2014. 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.[1]
- 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.[2]

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 first in a series of annual evaluations (up until 2018). Much of the data collection was carried out during the summer holiday period in 2015, which required an adaptation of the evaluation framework. More on the methodology, including strengths and weaknesses of the chosen approach, is presented in chapter 3. 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 framework in annex B)
Chapter 4: Description of ENISA's organisation, resources and procedures
Chapter 5: Findings of the evaluation
Chapter 6: Conclusions and recommendations
Chapter 7: Action plan

Complete survey results, the case study report for Cyber Europe 2014 and score board of achievements can be found in annexes.

[1] Decision No MB/2014/1 WP of the Management Board of the European Union Agency for Network and Information Security (ENISA) on the financial regulation applicable to the European Union Agency for Network and Information Security.

[2] 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

2. POLICY CONTEXT IN THE AREA OF NETWORK AND INFORMATION SECURITY

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 and establishment of ENISA

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[3]. In that same year, the Framework Decision on combating fraud and counterfeiting was adopted[4], which defined the fraudulent behaviours that EU States need to consider as punishable criminal offences. The following year – the ePrivacy Directive[5] was adopted, binding providers of electronic communications services to ensure the security of their services and maintain the confidentiality of client information.

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 deal with NIS, which encompasses both cyber security and Critical Information Infrastructure Protec (CIIP).

ENISA was tasked[6] 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[7].

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

[4] 2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment

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

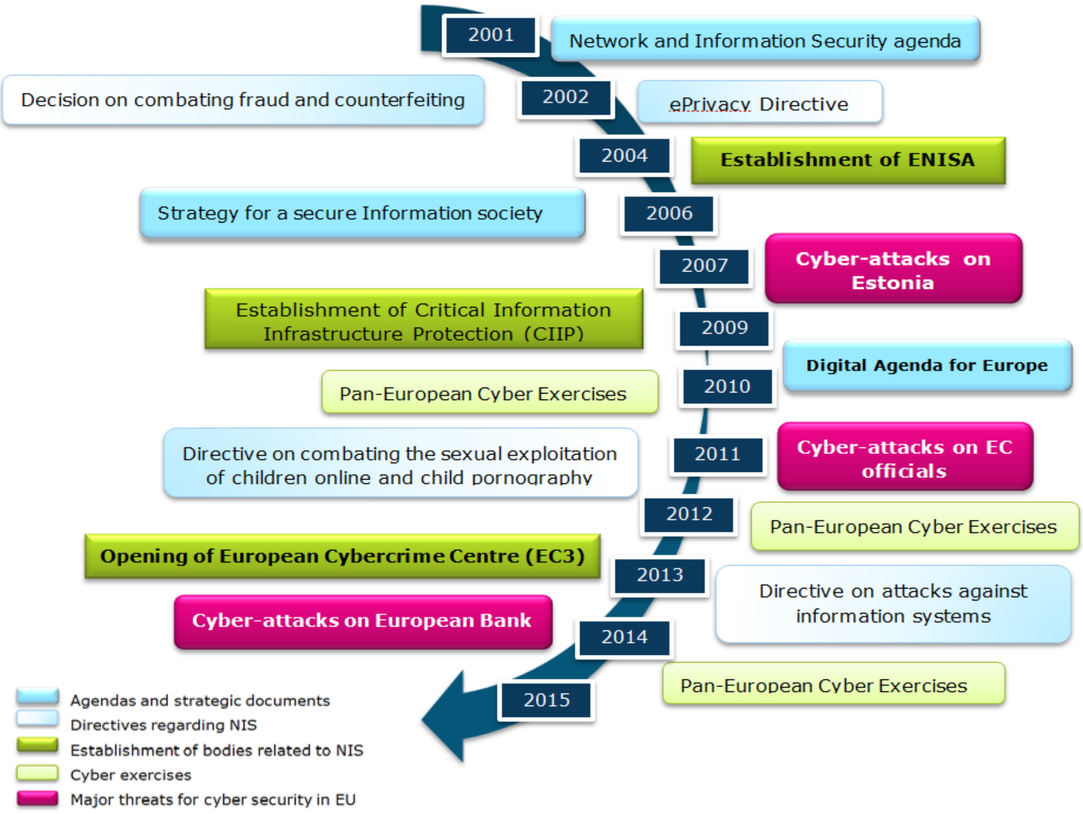
[6] Regulation 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the EuropeanNetwork and Information Security Agency.

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

After the large-scale cyber-attacks on Estonia in 2007, an EU initiative on CIIP was established in 2009[8]. 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.

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
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
Agendas and strategic documents
Directives regarding NIS
Establishment of bodies related to NIS
Cyber exercises
Major threats for cyber security in EU

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[9], which better addresses new developments in the online environment and the Directive on attacks against information systems[10] 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)[11], 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.

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

[9] 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

[10] 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

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

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[12]. 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[13] and serves as an umbrella for all EU conducted and coordinated activities in the field of NIS.

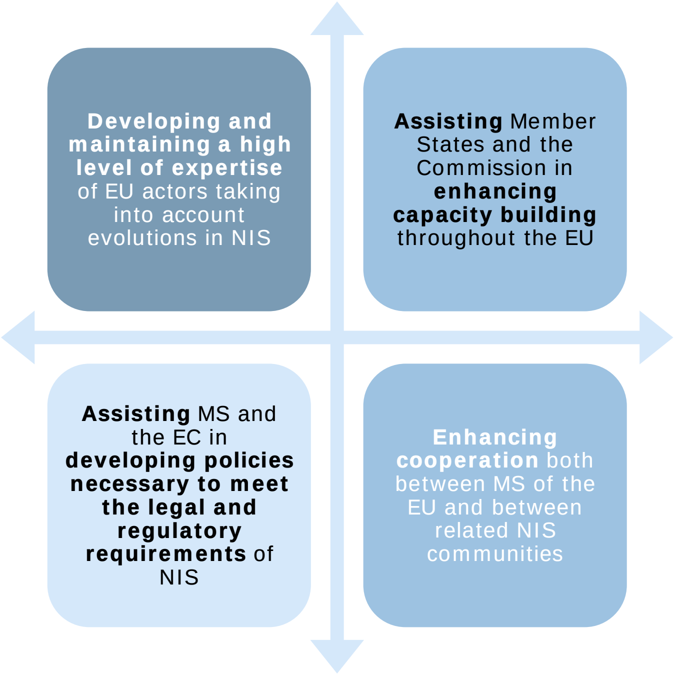
2.2 Legal background and mission

ENISA's legal basis can be found in Regulation (EC) No 460/2004[14], which established the Agency, two later extensions of ENISA's mandate, i.e. Regulation (EC) No 1007/2008[15] and Regulation (EC) No 580/2011[16], and, finally, the new ENISA basic Regulation (EU) No 526/2013[17] 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 (see more on governance in Chapter 4.1).

2.2.1 ENISA's objectives

In light of the previously described context of intensifying cyber treats, the Agency's objectives is enhance the capability of the European Union, the EU Member States and 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[18].

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

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

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

[14] 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)

[15] 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

[16] 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

[17] 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

[18] Objectives as agreed with the ENISA Management Board in the annual work programme 2014

Among other things, the Agency provides assistance to the Commission and Member States in their dialogue with industry to address security-related problems in hardware and software products. ENISA also follows the development of standards, promotes risk assessment activities 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 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.

2.3 The Agency's tasks and activities

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

- ✓ Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- ✓ Collecting and analysing data on security incidents in Europe and emerging risks.
- ✓ Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
- ✓ Awareness-raising and co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field.

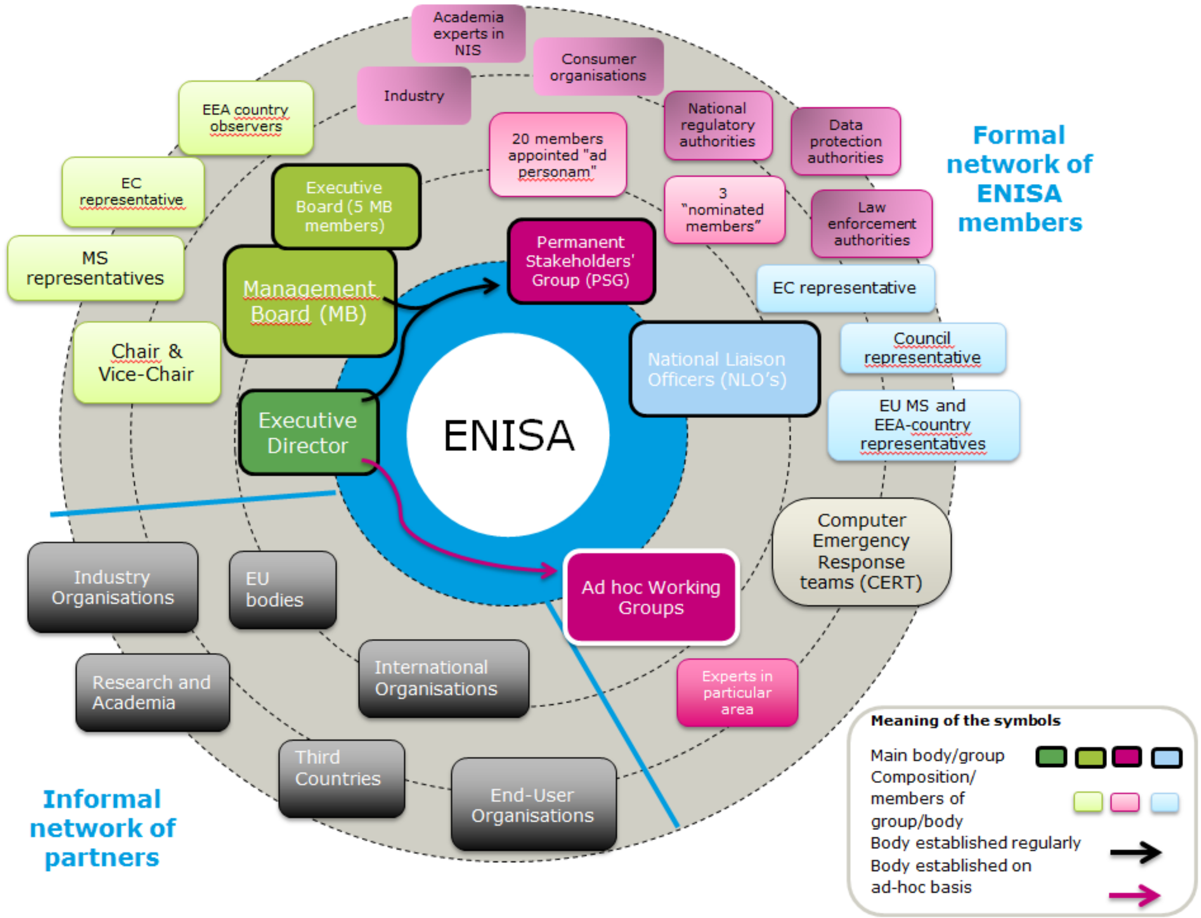
In addition, ENISA undertakes European NIS Good Practice Brokerage activities, which are based on the concept of the exchange of good practices between EU Member States at the area of NIS on a pan-European scale.

2.4 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 3 shows a map of ENISA's stakeholders who are vital and essential partners to its activities.

Figure 3. ENISA's stakeholder map

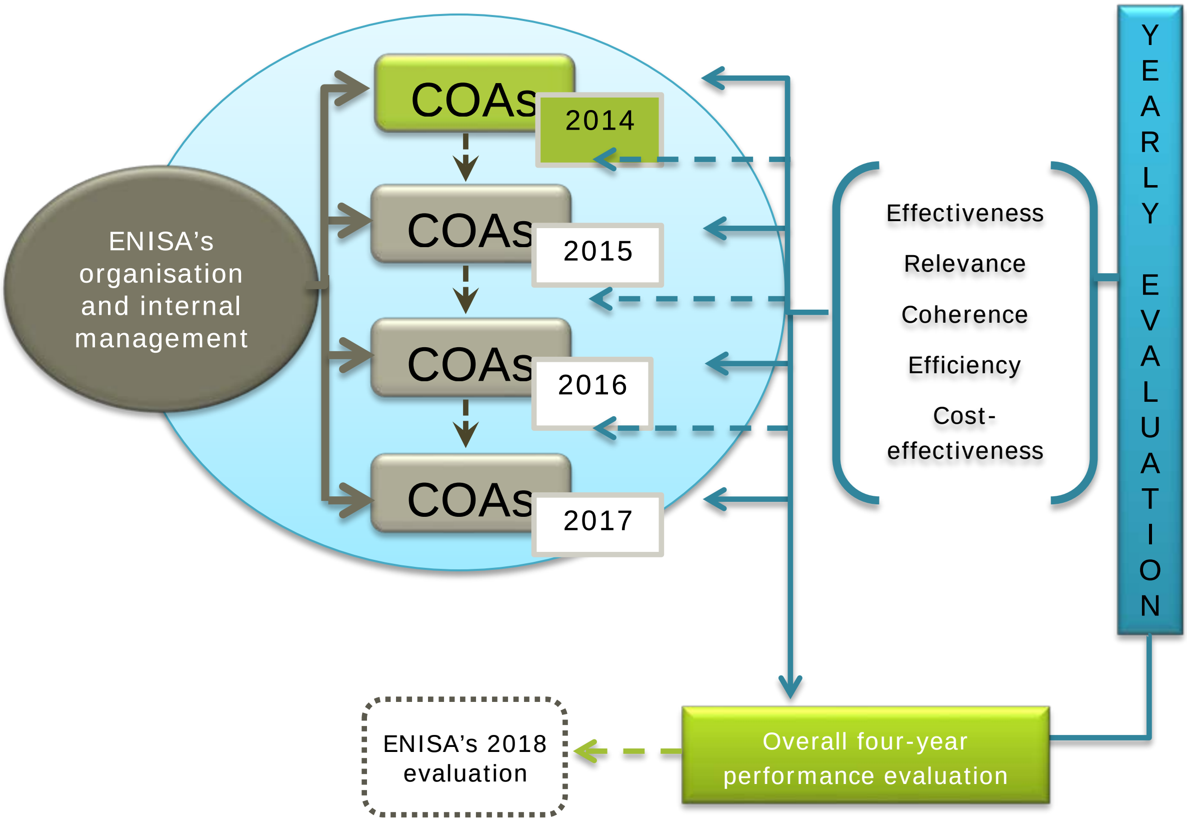

Academia experts in NIS
Consumer organisations
Industry
EEA country observers
EC representative
MS representatives
Chair & Vice-Chair
Executive Board (5 MB members)
Management Board (MB)
Executive Director
20 members appointed "ad personam"
National regulatory authorities
Data protection authorities
3 "nominated members"
Law enforcement authorities
Formal network of ENISA members
Permanent Stakeholders' Group (PSG)
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 OF THE EVALUATION

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

Figure 4: Our approach to the evaluation of ENISA's core operational activities



In order to meet the requirements, the evaluators have developed a two tier evaluation framework, one overall framework to be applied to all years being evaluated (evaluation questions matrix[19]) and one more detailed framework targeting the core operational activities for each year (2014 in this instance).

The evaluation matrices can be found in annex B, including a score board for the 2014 evaluation.

[19] 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.

3.1 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 2014 • Annual Report 2014 (draft) • Regulation (EU) No 526/2013 • Financial data from ENISA • Briefing documents developed by ENISA of staffing issues • Web statistics from ENISA
Interviews	• Group interviews with all Core Operational Departments (CODs) in Athens 16/07/2015
On-line survey	• On-line questionnaire to Management Board (MB) members and National Liaison Officers (NLOs), Permanent Stakeholder Group (PSG) and a sample of industry stakeholders
Case study on CE 2014	• Review of evaluation reports and follow-up actions • Interviews with a sample of involved stakeholders (7)

Data collection was carried out from mid-July to end September 2015. The process worked well, albeit with some expected delays due to the summer holidays. The support provided by ENISA to the evaluation exercise has been highly valuable and essential to reach 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 work streams in 2014. The MB and NLOs received the survey directly via e-mail from the evaluation team, while PSG/industry stakeholders received the survey via a link in an e-mail sent by ENISA. The number of respondents to the survey was limited, in particular for the MB/NLO respondents, despite prolonging the survey an additional two weeks until early September. That data collection took place during the summer holiday period may in part explain the meagre response rate.

Table 2 Response rates survey to stakeholders

Survey respondent group	Total sent	Total answered	Response rate
MB/NLO	86	29	34%
PSG/industry	53	34	64%
Total	139	63	45%

The data quality is judged as sufficient for analysis and conclusions, but should be interpreted with due consideration due to the limited number of responses (a broader and larger population of respondents would be necessary to ascertain validity of findings). 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 annex A.

A case study was carried out on Cyber Europe 2014 (CE2014). The case study is reported in a separate case report, see annex D, and its findings/conclusions have been integrated into relevant parts in the report. In coming evaluation periods, more case studies will be conducted (up to three per year).

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. Overall, it should be kept in mind that only a limited number of stakeholders have been reached in the evaluation of ENISA's 2014 core operational activities. While the findings are deemed reliable and valid, a larger sample and broader of stakeholders will be necessary to generate more robust conclusions on the achievements of ENISA. This should be taken into account in coming evaluation periods.

4. DESCRIPTION OF ENISA'S ORGANISATION

4.1 The organisation of the Agency

The bodies of ENISA comprise an Executive Director and staff divided between two departments, a Management Board, an Executive Board and the Permanent Stakeholders' Group. These are described below.

The Executive Director is appointed by the Management Board and is responsible for managing the Agency and performs his/her duties independently. He/she can establish ad hoc working groups, in consultation with the Permanent Stakeholders Group, which are composed of experts. The ad hoc Working Groups deal with specific technical and scientific matters.

The Management Board (MB) is composed of representatives of the Member States and the Commission. The tasks of the Management Board include the establishment of the budget, verification of its execution, adoption of the appropriate financial rules, establishment of transparent working procedures for decision-making by the Agency, approval of the Agency's work programme, adoption of its own rules of procedure and the Agency's internal rules of operation, as well as the appointment of the Executive Director. The Management Board will adopt the Agency's internal rules of operation on the basis of a proposal by the Commission. The Management Board ensures that the Agency carries out its tasks under conditions which enable it to serve in accordance with the founding Regulation[20].

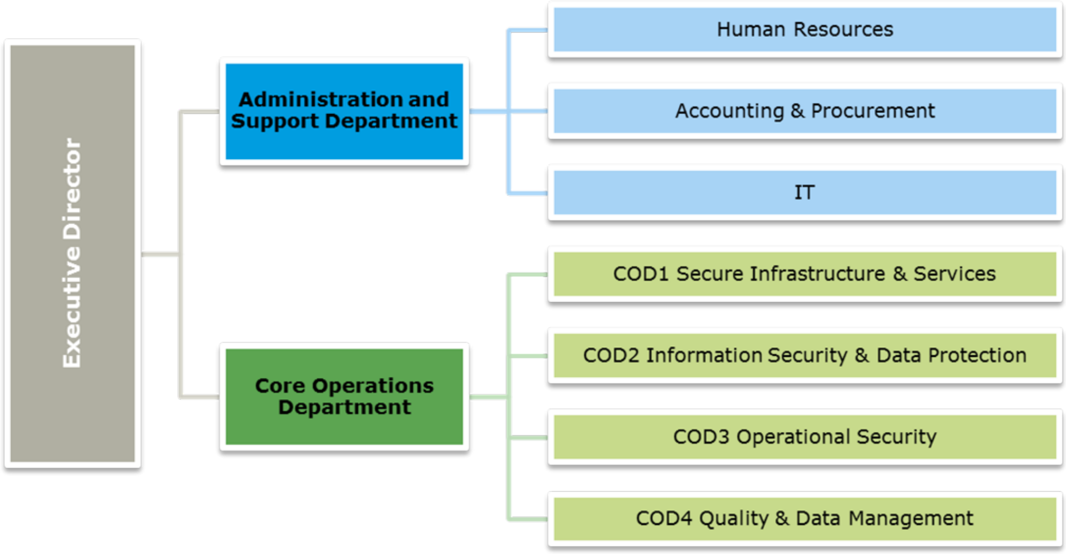
The Permanent Stakeholders' Group (PSG) is set up by the Management Board, acting on a proposal of the Executive Director for a term of office of 2.5 years. For the period 2015-2017, the PSG is composed of "nominated members" and members who are appointed "ad personam", representing in total 23 members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

In line with the operational and horizontal objectives of the Agency, ENISA's organisational structure was reorganised in December 2013. The current organisational structure, depicted in Figure 4 below, shows the two departments divided in three and four sub-units. They reflect the new challenges raised by the Agency's two locations, its stakeholders and the consequent need to address the changing operating environment with the limited number of human resources at the Agency's disposal.[21]

[20] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, repealing Regulation (EC) No 460/2004.

[21] ENISA Annual Report, 2013

Figure 5: ENISA organisational chart


Executive Director
Administration and Support Department
Human Resources
Accounting & Procurement
IT
Core Operations Department
COD1 Secure Infrastructure & Services
COD2 Information Security & Data Protection
COD3 Operational Security
COD4 Quality & Data Management

Source: ENISA website

The **Administration and Support Department** is located in Heraklion. Data collection with the department has not been foreseen for the evaluation of 2014 activities; therefore this department is not further described in the present report. Interviews with the employees of the administration should be considered for the next evaluation period.

The **Core Operations Department** (COD) is based in Athens. Work is divided among four units, COD1 to COD4. Each of the units is headed by a coordinator.

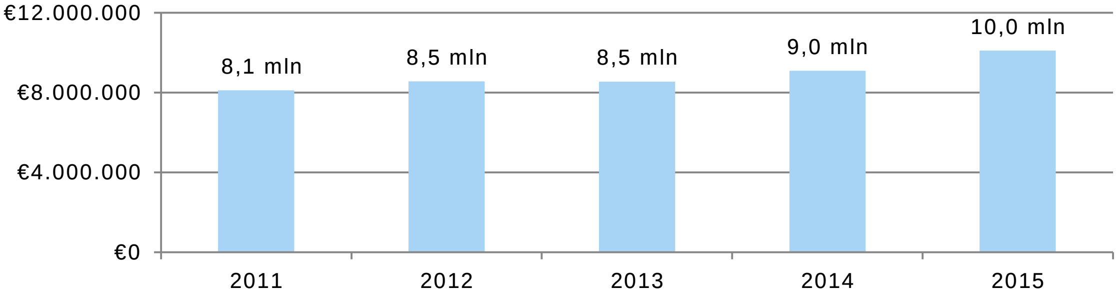
- **COD1** covers activities in the area of **Secure Infrastructure and Services**. The focus lies on business areas, such as telecommunication, finance or clouds in general. Also governmental networks and infrastructures are covered.
- **COD2** works on **Information Security and Data Protection**. The activities of the unit are the cyber security month, the area of cryptography and other privacy and data protection activities such as support to the Commission on the implementation of the e-ID action plan. Until the end of 2014, cyber exercises were also conducted by COD2.
- The cyber exercises have now moved to **COD3** which is named **Operational Security**. This unit also covers the work on CERTs which includes studying baseline capabilities, providing trainings for Member States and the evaluation of ENISA's impact in this field.
- **COD4 Quality and Data Management** provide horizontal support to the other units in particular in the area of quality management but also in terms of communication and collaboration with stakeholders. It was only set up in the last quarter of 2014.

The financial rules of ENISA are laid out in ENISA's Financial Regulation 2014[22], which repealed the Regulation of 2009. It identifies the Management Board as a main internal body of the Agency, responsible for taking decisions on financial and budgetary matters. The Executive Director is regarded as an authorising officer responsible for implementing the decisions of the Management Board and the budget of the Agency. The budget of the ENISA comprises a contribution from the EU Budget which over years constitutes around 90% of the Agency's revenue, rent subsidies from the Government of the Hellenic Republic (in 2014 constitutes around 7%), as well as contributions from third countries participating in the work of the Agency (around 3% in 2014).

[22] DECISION No MB/2014/1 WP Of the Management Board of the European Union Agency for Network and Information Security (ENISA) on the financial regulation applicable to the ENISA in conformity with the Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council

In 2014, the Agency had a budget of 9.0 million Euros. Figure 5 shows the annual increase in ENISA's budget. The overall increase in five years is around 2m EUR or an increase of 24.6% relative to the 2011 budget.

Figure 6 ENISA's budget 2011-2015



Source: ENISA's Statement of Estimates (Budget 2011/2012/2013/2014/2015)

In terms of budget execution, the expenditure appropriations corresponding to the Union contribution allocated to ENISA and the interest generated by cash at banks during 2014, i.e. the Budget of ENISA of 9,091,917.98 EUR, were committed at a rate of 100% on 31/12/2014 compared to 99.72% on 31/12/2013. The respective payment rate on EU subsidy expenditure appropriations as included in the MFF 2014-2020 was 85.61% in 2014 compared to 91.32% in 2013.[23]

Staff cost is the main expenditure for ENISA, with about 60% of the budget allocated to staff, 23% to operations and 17% to administration. At the end of 2014, 62 statutory staff were employed by the Agency. The evolution of staff since 2011 is shown in the table below, which reflects a relative stable number over the period and a marked (planned) increase in 2015[24].

Table 3 Staff by category end of year

Staff category	2011	2012	2013	2014	2015 (planned)
AD	26	27	27	30	32
AST	15	15	16	16	16
CA	13	12	13	14	24
SNE	4	4	3	2	3
Total	**58**	**58**	**59**	**62**	**75**

During the interviews it was stressed by ENISA that recruiting and retaining qualified staff is a challenge for the Agency. By end 2014, the estimated turnover ratio was at 15%, according to a briefing paper elaborated by ENISA to describe the recruitment challenges. In particular it has proven difficult to recruit qualified expatriate staff, due to relatively low salary levels (compared to industry) and the living situation in Greece, with very expensive international schools in Athens, and one school in Heraklion providing education in English.

In coming years it is foreseen that ENISA should recruit an additional 10 Contract Agents (CA) to the operations area. These positions are difficult to fill with the current salary level (basic level for the functional area concerned is 2,476.74 EUR according to vacancy announcements) and limited benefits or allowances. As a consequence, most applicants are either Greek nationals and/or from other parts of Southern Europe, with very few applicants from northern Europe. This

[23] Annual Activity Report 2014

[24] Data from annual/general reports 2011-2014.

is also reflected in the current staff composition of the Agency, with approximately 34% of staff being Greek nationals, and few from northern parts of Europe[25].

According to the interviews with ENISA staff, the difficulties in recruiting and retaining the right staff mix can become detrimental to the Agency's work as a mediator of expertise and knowledge in NIS. For the Agency to fulfil its role, it needs to have access to high level expertise and sector knowledge in order to engage effectively with the NIS communities in Europe.

The interviews further revealed that the recognition of ENISA's activities is often seen through its ability to collaborate with external partners. This includes being recognised by other EU institutions, becoming known outside EU structures, having deliverables referenced or being invited to events. Similarly, the set Key Impact Indicators (KIIs) focus on the involvement of stakeholders in activities and the references made to ENISA's work. External communication with experts furthermore allows ENISA staff to keep abreast of latest developments in their area of work such as recent threats and developments in technology. This further underlines the need for high level expertise in the Agency.

4.2 Management systems and procedures

ENISA's work is based on annual planning. The work programmes are set up in consultation with ENISA's PSG and the Management Board. Member States provide comments on the programme. The work is structured in Core Operational Activities which in 2014 were divided across three work streams. Additionally, Horizontal Operational Activities are conducted. KIIs are set for the activities to evaluate long-term performance and link them to the strategy of the Agency. They are followed up with annual activity reports.

ENISA staff uses the MATRIX project management system for their project management. Staff book their hours in the system and it provides an overview of resources for each project. MATRIX automatically generates reports for the management on a biweekly basis. However, the system is not considered relevant for generating management information at an operational level, and it is not used actively to steer projects. Instead, in addition to MATRIX, there are spreadsheets used by each COD unit to maintain an overview of projects on a daily basis. These sheets are individual to each unit and vary in content from one unit to another. During the interviews, ENISA staff indicated that the MATRIX system did not provide for sufficient functions for project management at COD unit level, such as tracking risks and issues. For this reason the spreadsheets have been set up. There are plans to standardise the spreadsheets in the future.

Quality assurance of projects is done with a Quality Management System (QMS). A range of instruments is available to ensure quality such as manuals and guidelines laying down standard operating procedures. According to interviewees, the tools are widely used among the staff. Activities follow the Deming Cycle (plan, do, check, act).

4.3 Collaboration and communication

Structures to ensure collaboration and communication between the employees of ENISA are in place. As the Agency's activities are set up according to the work streams by the Management Board and the PSG, not taking into account the structure of CODs, cooperation between the different units is important. In this context, it is very beneficial to be in the same building. However, employees noted during the interviews that there were synergies that could be better taken advantage of and that it was difficult to stay informed about the work of all units considering time constraints. The fact that ENISA's Administration and Support Department is not located in the same place as the operational units creates obstacles to cooperation despite efforts to hold weekly virtual meetings.

[25] Annual report 2014

5. FINDINGS OF THE EVALUATION

The findings of the evaluation are structured around the evaluation criteria defined in the terms of reference. The findings present the overall relevance, impact and efficiency of ENISA's activities, and look more in detail at achievements in relation to the work streams and core operational activities carried out in 2014, in terms of effectiveness (achievement of objectives). Throughout the presentation, findings are triangulated (comparing different sources of information) and a part conclusion is provided.

5.1 Overall relevance of ENISA's activities

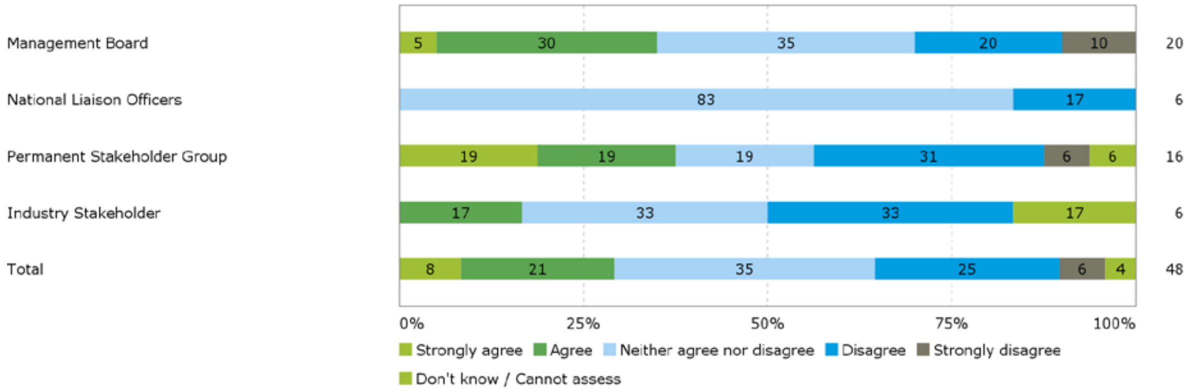
The assessment of relevance relies on analysing the linkages between core operational activities and ENISA's legal mandate, and if there has been a balance in addressing different tasks. Furthermore it is based on stakeholder's opinions of whether activities are responding to needs in the EU and Member States, and on the extent to which the actual outputs have been useful (utility).

Overall, there was a clear linkage between the core operational activities carried out in 2014, and the legal mandate of ENISA. It can be concluded that while all tasks stipulated in the Regulation were addressed, there was a focus on cooperation activities and on capacity building, as per the definition in the legal framework, with activities such as CERT training and cooperation, guidelines for private and public stakeholders, Cyber Exercise 2014 etc. being carried out. No specific core operational activity was carried out in relation to Article 31 (f) *contribute to the Union's efforts to cooperate with third countries and international organisations to promote international cooperation on network and information security issues*. However, since the evaluation only covers deliverables with a budget above 30,000 Euros, cooperation with third countries and international organisations has taken place with smaller budgets and as a part of operations.

One minor observation relates to the objectives of ENISA, whereby the Regulation states in Article 2.2 that *"The Agency shall assist the Union institutions, bodies, offices and agencies in developing policies in network and information security"*. Looking at the core operational activities in 2014, this does not seem to have been pursued specifically, with no activities targeting Union bodies explicitly. However, this takes place in other activities, for example CERT EU took part in Cyber Exercise 2014, and a specific strategic level exercise was conducted by/with the Council, as a spin-off from Cyber Exercise 2014, using ENISA's approach and support.

In the survey, stakeholders were asked if cyber security challenges are adequately addressed in the EU and in the Member States. It is clear from responses that a majority of respondents were either neutral or negative, with the MB being somewhat more positive. Still, based on the responses, it can be concluded that stakeholders perceive that much remains to be done to ensure NIS and cyber security, as illustrated in Figure 6 below.

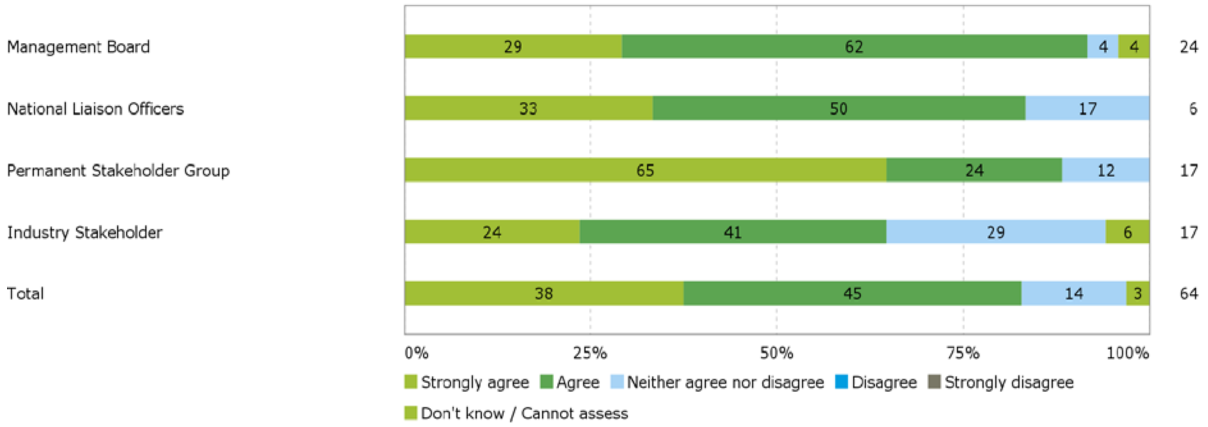
Figure 7 Q3.8 Cyber security challenges are adequately addressed in the EU



A similar question looking at whether security challenges are adequately addressed at the Member State level revealed that 43% disagreed/disagreed completely to the statement (survey annex Q3.9).

In the survey, a clear majority of stakeholders, 84%, agreed that ENISA's scope and objectives correspond to the needs for NIS in EU (clearly above threshold of 70% agreeing[26]), which is a strong finding in light of the stated need as indicated previously. Results were similar regarding whether it corresponds to needs in the Member States (survey annex Q1.1).

Figure 8 Q1.2 The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the EU



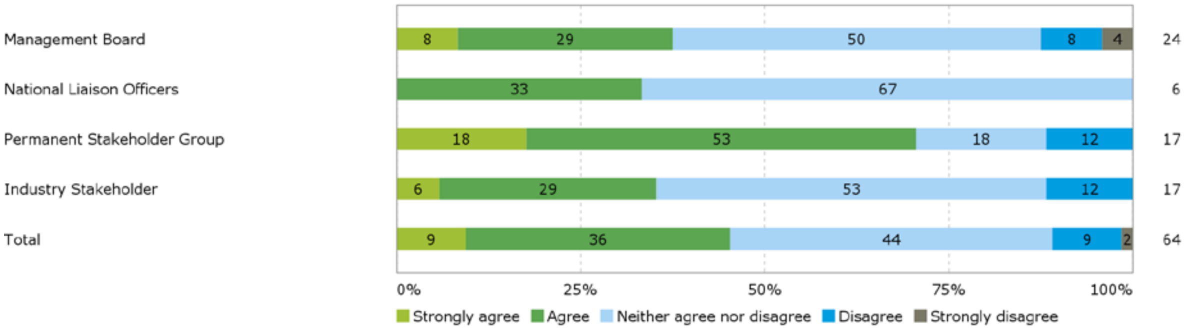
There are minor differences in rating between different stakeholder groups, but overall the responses were positive. Among industry answers, there was less agreement on the outputs of ENISA corresponding to the needs in Member States and the EU. In open comments, this was further elaborated as being linked to the responsiveness of decision makers, as well as limited mandate and resources of ENISA, as illustrated by the following quotes from the survey.

- *I think the ENISA work is very relevant at EU level. I also think that the ENISA work is relevant at Member States level but could be even more relevant if there was political will from the Member States (PSG/Industry)*
- *Resource limitations and restrictions in the mandate reduce the effectiveness of what could be achieved (MB/NLO)*

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

Overall, the stakeholders agreed that ENISA effectively meets the expectations of stakeholders (survey annex Q1.6). However, it does not seem to be entirely clear to respondents what ENISA expects of stakeholders. Respondents were neutral or possibly uncertain, apart from in the PSG, where most respondents seemed to have a clear understanding of expectations.

Figure 9 Q1.7 It is clear what ENISA expects from stakeholders



Again the open answers make a connection to the mandate of ENISA and the context in which the Agency operates, as illustrated by the quotes below, both from the PSG/Industry survey.

- *ENISA could better meet expectations if it would be allowed to have a wider role. (PSG/industry)*
- *Information security has a lot of stakeholders. I think ENISA is challenged to reach all of them and it is difficult to meet their expectations. (PSG/industry)*
- *Many stakeholders would be open to greater participation in the areas of their expertise if it were congruent with ENISA's charter. (PSG/industry)*

The interviews conducted as part of the case study on Cyber Europe 2014 (CE2014) further suggest that ENISA has an important role to play within the area of cyber security, notably as “a trusted broker”, an advisory body and in terms of the organisation of EU-level cyber exercises. ENISA “should continue what it is doing” as “what they do is good”; ENISA brings together the opinions and experiences of EU countries / cyber crisis agencies to raise awareness, educate, share lessons learned, and it also supports the streamlining of cyber security procedures throughout the EU. It was suggested that its role could be increased to act as a coordinator, creating technical capacities and providing 24/7 technical support on the basis of cyber security information being shared with it by Member States as “the current structures lack the type of leader that ENISA could be”, with the EU CERT playing this role for the EU institutions alone.

Based on the findings, it can be concluded that ENISA clearly responds to a need in the European NIS landscape. The scope and objectives of ENISA’s work is seen as relevant to respond to the needs, but 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.

5.2 Overall 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.

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.

The responses in the survey were largely positive; above 70% agreed to the statements in all three questions. In particular the statement on raising awareness was strongly supported by 81% of the respondents (survey annex Q5.2), and the other statements were supported by around 70% (survey annex Q5.1 and Q5.3). This can be considered a quite strong finding on the likely contribution of ENISA to the more overall objectives that fall within the Agency’s mandate.

Industry stakeholders are somewhat more negative in their assessment of impact, with industry respondents agreeing to a lesser extent (below 70%). The actual number of industry respondents was small, so interpretations should be made with caution, but in some of the open answers the rationale for the rating was further clarified.

In open comments, this assessment was further explained by the PSG/industry respondents:

- *ENISA's facilitation role restricts its ability to meet ambitious objectives.(PSG/industry)*
- *ENISA does not have enough funding to achieve EU society in general to build up a culture of NIS or raising awareness. (PSG/industry)*
- *This is very important. I think it's too little. Just having a cyber-security month is not sufficient. (PSG/industry)*

In the interviews with ENISA staff and management, reference was also made to the perceptions/opinions expressed by stakeholders. As the Agency is working mainly for and through its stakeholders, with a limited budget and staff resources, direct impact should not be expected according to interviewees.

In conclusion, it appears that despite ENISA’s limited mandate and also fairly small resources, the Agency manages to make a real contribution towards increased NIS in Europe, as perceived by key stakeholders.

In the subsequent section on the effectiveness of ENISA’s work, the evaluation looks into the key achievements under the 2014 Work Programme.

5.3 Effectiveness of ENISA’s activities: Evaluation findings related to 2014 Work Streams

In the 2014 Work Programme, activities were structured around three work streams, each containing three work packages and a number of deliverables. The deliverables correspond largely to what are called core operational activities. This evaluation of effectiveness covers all core operational activities implemented in 2014, with a budget over 30,000 Euro.

The core operational activities in 2014 were structured along three work streams:

- WS1: Support EU policy building
- WS2: Support capacity building
- WS3: Support co-operation

The information in this section is based on the Work Programme and Annual Activity Report 2014, as well as assessments from the stakeholders in the survey. It is complemented with the views shared by the staff of the four CODs during group interviews and further documents analysed in a desk review. A more in-depth case study has been conducted on the 2014 Cyber Exercise; the findings of the case have been integrated into the analysis where relevant, in particular under WS3: Support cooperation.

5.3.1 Achievement of Key Impact Indicators (KII) and statistics on downloads

The KIIs set in the 2014 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 annex A.

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 700,000 times. The most downloaded reports were “Cloud Computing - Benefits, risks and recommendations for information security” from 2009 (44,850 downloads) and the “Good Practice Guide for Incident Management” from 2010 (36,585 downloads).

When looking specifically at the reports published as a part of the 2014 Work Programme, of which many were published in Q1 2015, the total number of downloads was 155,762 as at June 2015. Since the length of time for which the reports had been available online was very short at the time of writing, it is not possible to make a firm link between the number of downloads and the presumed “success” of a deliverable.

The report with the highest number of downloads, with around 21,000 downloads, was the report “*Privacy and Data protection by design*”[27], followed by 13,000 downloads for the report “*ENISA Threat Landscape report 2014*”. Other reports with a high number of downloads (above 7,000) include (in order of downloads); “*An evaluation framework for Cyber Security Strategies*”; “*Algorithms, key size and parameters report 2014*”; “*Cloud security guide for SMEs*; and *Security framework for governmental clouds*”. The reports with the smallest number of downloads related to the CERT baseline capabilities and guidelines on secure ICT procurement. For all deliverables included as core operational activities, the number of downloads can be found in annex A.

The evaluation can conclude that some of ENISA’s deliverables have generated a high number of downloads in a short period of time (most reports were made available in Q1 2015 and thus downloads had only been available for a few months at the time of writing). In subsequent evaluations, it is suggested to systematically follow up on the numbers of downloads to track developments over time.

[27] WPK 1.2: D4. Not included in the list of Core Operational Activities >30,000, and therefore not included specifically in the evaluation of core operational activities.

5.3.2 Work stream 1: Support EU policy building

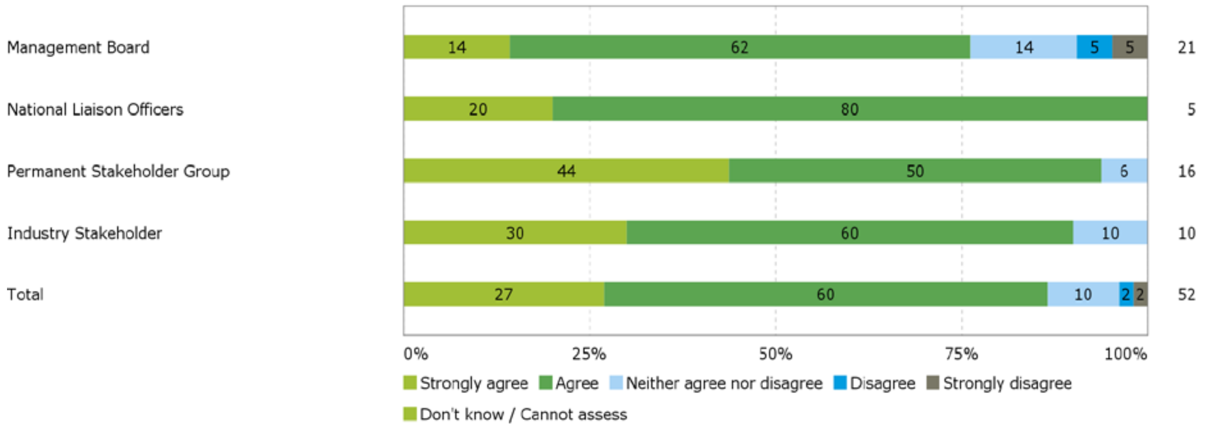
With work stream 1, ENISA sets out to support the development of EU policy in the field of NIS. This was to be achieved through developing and maintaining a high level of expertise, facilitating voluntary information exchange, establishing mutual interactions, contributing to EU policy initiatives, and supporting the EU in research and standardisation.

5.3.2.1 Work package 1.1 Identifying evolving threats, risks and challenges

The objective of this work package was to collect data on current threats to NIS. It included two deliverables relevant for this evaluation. The ‘Annual EU Cyber Security Threat Landscape’ (D1) and ‘Identification of trends, security challenges, associated risks and required countermeasures for emerging technologies’ (D2). The threat landscape is based on existing publicly available material on current and future threats and risks. Based on the interviews undertaken, the quality of collected information on threats has improved compared to previous years. The aims with regards to references by Member States and stakeholders to ENISA publications under this work package were largely achieved.

Almost all survey respondents confirm that the work undertaken by ENISA to identify threats, risks and challenges has been relevant and of high quality, 87% in total.

Figure 10 Q2.2 ENISA’s deliverables about NIS threats in the EU are relevant and of high quality



This is a very strong finding, confirmed also by the achievement of KIIs and interviews.

5.3.2.2 Work package 1.2 Contributing to EU policy initiatives

With work package 1.2, ENISA intended to provide input to new policy initiatives and to assist the European Commission and the Member States in implementing such initiatives with a NIS perspective. The deliverable ‘Algorithms and parameters for secure services’ (D3) was developed. It is an initiative which has been running since 2013 works on developing technical specifications for cryptographic algorithms to protect personal data in e-government services. ENISA published a best practice guide in this field and updated recommendations developed in the previous year. Support for these activities was wide spread, coming from competent authorities in the Member States, as well as known experts in the field.

Survey results from stakeholders confirm the assessment from the KII follow-up, with above 70% agreeing to the statements regarding usefulness of ENISA’s input to the development and implementation of new policies for NIS in EU and Member States (survey annex Q2.4 and Q2.5).

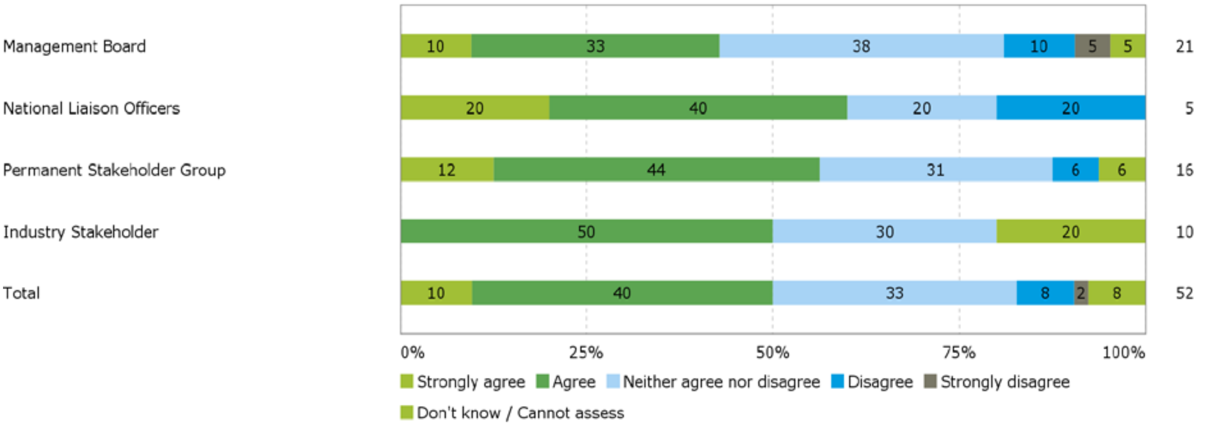
5.3.2.3 Work package 1.3 Supporting the EU in education, research and standardisation

In its effort to support standardisation and EU funded research and development initiatives, ENISA developed an ‘Inventory of standardisation in NIS and Privacy’ (D1) through workshops and reports. The support received from Member States in these activities exceeded the set aims and the various scenarios developed throughout 2014 will be further implemented in 2015.

The contribution of ENISA to putting in place more effective mitigation strategies and to setting standards for NIS and privacy was rated by stakeholders as less certain, just below 70% (survey annex Q2.7 and Q2.9). On the relevance of information provided by ENISA to stakeholders on standardisation, innovation and research, the answers were also mitigated, with 65% agreeing/strongly agreeing (survey annex Q2.6).

Finally, about 50% agreed/strongly agreed that ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services.

Figure 11 Q2.8 ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services



In open answers, the respondents further elaborated on ENISA's support to EU policy, mainly emphasising the need for cooperation and coordination between stakeholders involved in the policy development.

- *ENISA's work at EU level needs further effort and coordination. (MB/NLO)*
- *ENISA should be focused on building capacity and capability in the EU, rather than providing deliverables about NIS threats. The Commission should consult ENISA more thoroughly before making announcements about NIS policy (e.g. the PPP announced in the DSM communication). (MB/NLO)*
- *I do not see ENISA helping Members (states) to develop their policies. (PSG/industry)*
- *Still a lot of work in progress but ENISA should remain the reference within the EU. (PSG/industry)*

The evaluation findings show that the work conducted under work stream 1 has been successful in achieving most objectives. In particular the work conducted in identifying evolving threats, risks and challenges, and the contribution to EU policy initiatives appear to have achieved intended results. For the work done in supporting the EU in education, research and standardisation, results were more mixed, in particular regarding the link to actual operational issues such as data protection and secure services. These aspects are evidently not under the direct control of ENISA but national regulators and operators, hence the need for further efforts in coordination and cooperation.

5.3.3 Work stream 2: Support capacity building

This work stream is aimed at increasing the capacity of Member States and industry in the protection of critical information infrastructure from cyber-attacks or disruptions. Note that work package 2.3 focuses on awareness raising among citizens and comprises the European Cyber Security Month, but did not cover any deliverables with a budget of over 30,000 EUR to be assessed within this evaluation.

5.3.3.1 Work package 2.1 Support Member States' capacity building

ENISA supports the development of prevention, detection, analysis and response capabilities of Member States and EU institutions. Under this work package three deliverables were relevant for the evaluation. A 'White Paper on How to Evaluate National Cyber Security Strategy' (D2) was to be developed. ENISA took stock of existing assessment mechanisms for cyber security strategies. To this end a working group was set up comprising more Member States and private companies than initially targeted.

Within this work package, ENISA conducted capability building with national or governmental CERTs which focused on suitable exercises for technical staff from Member States, EU institutions and other audiences. The aim is to level capabilities across Europe as they vary strongly between the countries. A 'New set of CERT exercise material with at least five new scenarios from the four areas of the "baseline capabilities"' (D5) was noted as a deliverable.

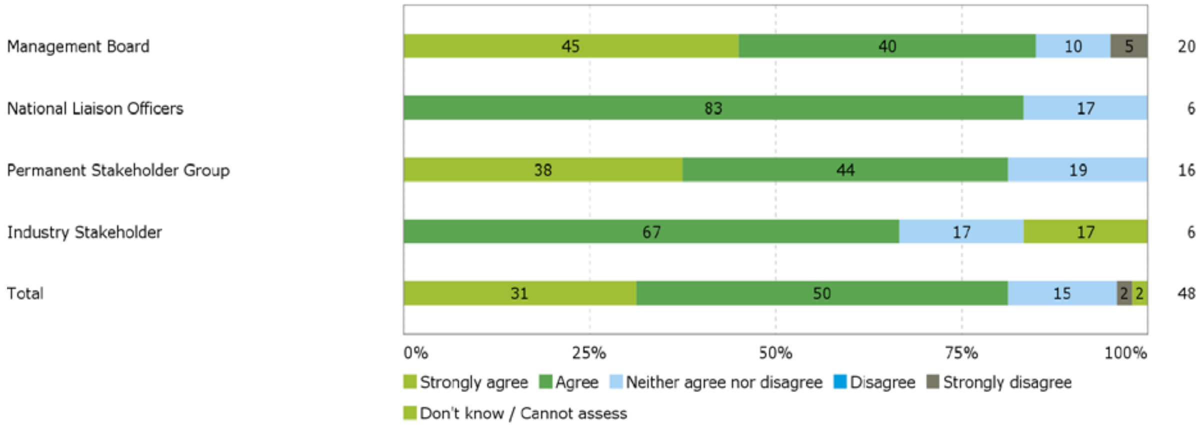
The CERT trainings were very successful with the participation of more than 135 people, compared to an original target of 20. The deliverable 'Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work in this area' (D6) reviewed lessons learned from the past eight years of working with CERTs. This was done in a close dialogue with relevant stakeholders. None of the KIIs set out in the Work Programme were to measure achievements.

ENISA published an impact assessment on "Supporting the CERT Community" which came to the conclusion that the Agency's role and impact is recognised across the Union. ENISA has the potential to become a representative voice for CERTs in the European context. Stakeholders are well aware of the Agency's activities, which are positively perceived. Knowledge about ENISA could be improved among private sector CERTs. It was suggested that it may be worth considering splitting training sessions between advanced CERT experts and beginners. ENISA could furthermore become active in investigating trends and threats in greater depth and translate conclusions and recommendations in several languages. The focus of ENISA on supporting harmonisation and setting common standards among CERTs was supported.[28]

Survey results show that stakeholders consider that ENISA has contributed to developing capacities in Member States, with 81% agreeing/strongly agreeing.

[28] ENISA (2014): Supporting the CERT Community "Impact Assessment and Roadmap", Version 1.0

Figure 12 ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States



A further 85% agree/strongly agree that good practices in NIS have been disseminated by ENISA (survey annex Q3.2).

It can be concluded that the survey results related to capacity building in Member States are very strong and consistent, indicating that ENISA effectively carries out this part of the Agency's mandate.

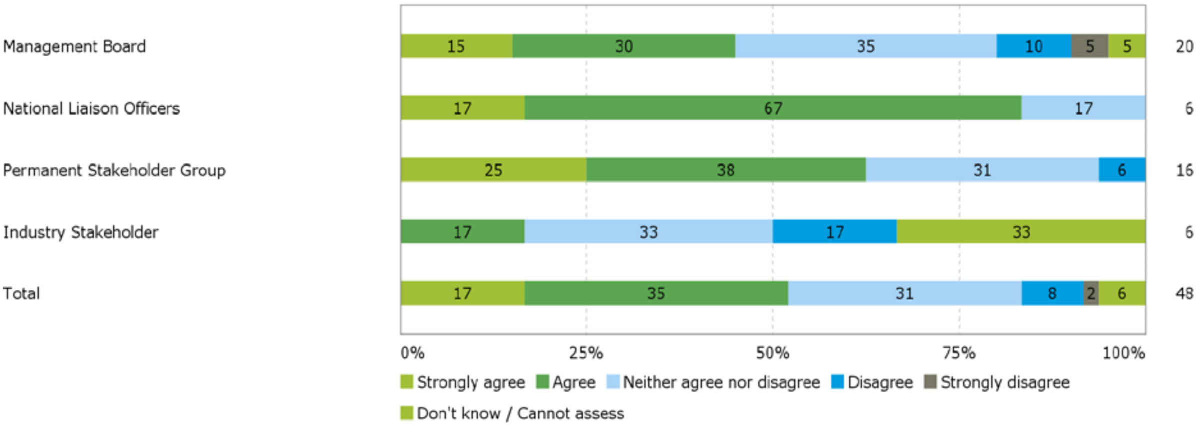
5.3.3.2 Work package 2.2 Support to Private Sector Capacity Building

Under this work package, ENISA focused on enhancing the capabilities of the private sector through cooperation with the public sector in different fields such as financing, electronic communication networks and smart grids. The state of preparedness in the event of large-scale cyber incidents was to be improved. The support to the private sector included five deliverables with a budget of over 30,000 EUR. A 'White Paper on the Certification of Smart Grids' (D2) was developed, and for which a validation workshop was conducted. None of the KIIs for this work package would measure the achievements of this deliverable. Another report, the 'White Paper on the Certification of Cyber Security Skills of ICS SCADA experts' (D3) was defined as a deliverable. It provided recommendations for developing harmonised certification schemes at European level for the skills of these experts. ENISA has successfully set up a working group with experts from utilities manufactures vendors and public authorities in this area, which was set as one of the targets. 'Minimum Security Measures for Cloud Computing' (D5) were laid down in a meta framework. This supports cloud certification activities for the EC Cloud Strategy.

The number of stakeholders targeted to participate in the study was overachieved. For the deliverable 'Guidelines for the identification of critical services, assets and links in electronic communication networks' (D7), no relevant KIIs were included in the Work Programme. The activities on electronic communications include a group of providers who work on a harmonised framework for minimum security measures. Also 'Guidelines for secure inter-banking communications and transactions' (D8) were developed. The Agency worked together with national banks and identified areas for improvement and gave recommendations in order to increase the security of financial transactions. The number of experts in IT and the finance sector targeted by the activity were involved in the study published under this deliverable.

Survey respondents were less positive regarding ENISA's contribution to improving preparedness in the private sector to respond to NIS threats or incidents (below the norm 70% set for the evaluation).

Figure 13 Q3.4 ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or incidents



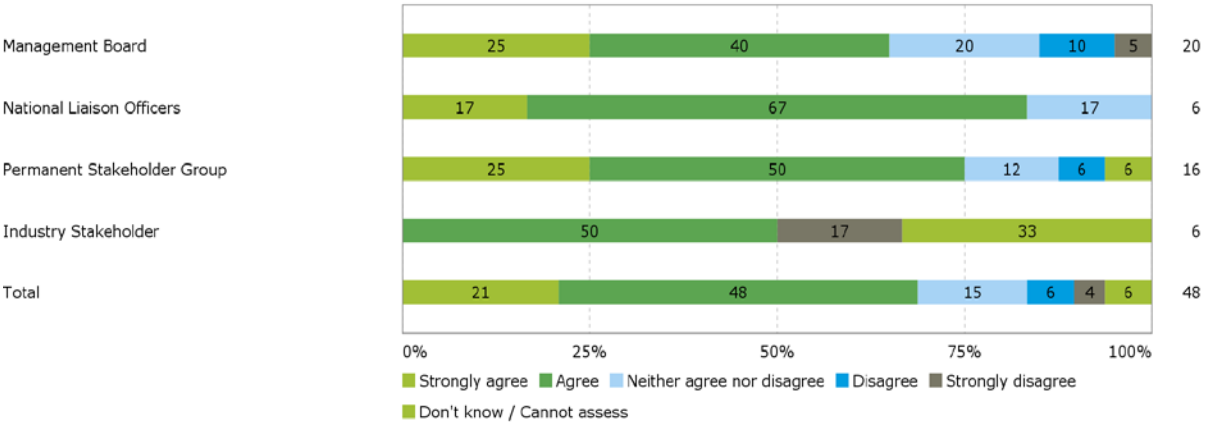
A few comments in the open answers from PSG/industry respondents elaborate on this, as presented below.

- *Private Sector stakeholders in my Member State, dominated by SMEs, are largely ignorant of ENISA and the good practice recommendations. Direct EU outreach arrangements would be more effective. (PSG/industry)*
- *Knowledge about ENISA is too low in the private sector. Parts of public sector. (National CERT, Telecom).*
- *There is a need for a more clear (communicated) cyber security strategy and roadmap on both EU and member state level. If there are strategies, they have to be communicated more. (PSG/industry)*

The potential group of private stakeholders is vast and heterogeneous, which makes it difficult for ENISA to reach out effectively with the resources at its disposal.

However, on the more overall and operational question on whether sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA, 69% of respondents agree/strongly agree (almost at threshold 70%). Although responses vary between the different stakeholder groups, the finding seems consistent.

Figure 14 Q3.7 Sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA



To conclude on work stream 2, ENISA's work to develop capacity in Member States (to coordinate and cooperate during crises, and the support to develop capacities and strategies at Member State level) has been successful in achieving the objectives. The contribution to private sector capacities looks more uncertain, based on the responses from the stakeholder survey.

5.3.4 Work stream 3: Support co-operation

The focus of work stream 3 lies in supporting the implementation of EU legislation related to NIS, as well as supporting cooperation between all stakeholders of the NIS field. ENISA builds on existing collaboration and enhances community building in Europe.

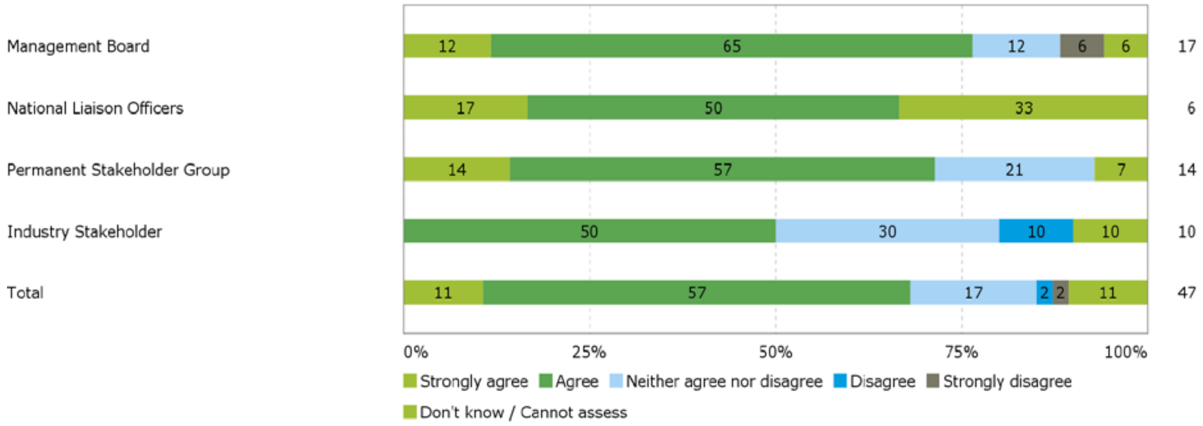
5.3.4.1 Work package 3.1 Crisis cooperation - exercises

This work package covers the preparation, implementation and follow-up of the Cyber Europe Exercise. The work was split between two deliverables: 'Cyber Europe 2014: Exercise Plan and Exercise' (D1) and the 'Report on Cyber Crisis Cooperation and Exercise Activities and Findings' (D2). The exercise was more ambitious than in previous years in terms of scenarios, the stakeholders involved and overall complexity. The results in terms of involved experts and participating Member States were above the set targets.

ENISA conducted an evaluation of the Cyber Europe 2014 (CE2014) exercise, comprising observations during the exercise, post-exercise participant surveys, and two workshops, the results of which are presented in an After Action Report; these results are explored in detail in the CE2014 case study report in annex D.

The goal of CE2014 was to train Member States to cooperate during a crisis, with the shared objective to mitigate large-scale cyber security incidents. In the survey, stakeholders were asked whether ENISA's support has improved services, workflow and communication among stakeholders to respond to crisis, to which 68% agreed/strongly agreed (close to 70% threshold).

Figure 15 Q4.6 ENISA's support has improved services, workflow and communication among stakeholders to respond to crises



The survey question did not relate specifically to CE 2014. However, the case study on CE2014 supported these results, suggesting that C2014 has led to improvements in Member States' workflows and communication to respond to emergency cases at national level in that they allowed for national NIS contingency plans and capabilities to be tested and technical gaps to be identified, where relevant, and led to concrete action being taken at national level in relation to any weaknesses identified. However, the exercises also served to identify weaknesses in the level of alerts and exchanges of information, and the level of secure means with which to so do, suggesting that there is still a long road ahead before an EU-level crisis management process is put in place.

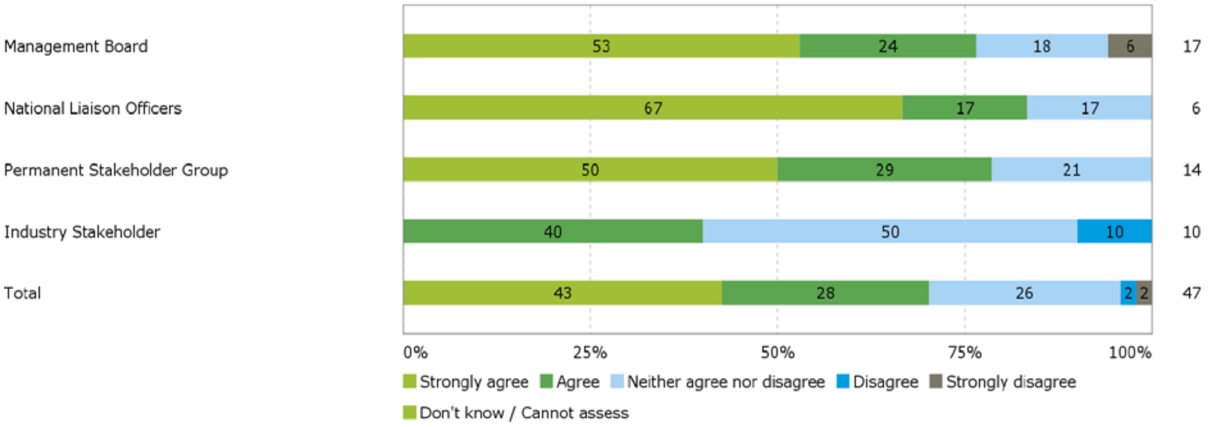
In a similar question, the assessment from stakeholders was slightly more positive, with 72% agreeing/strongly agreeing that ENISA's support has enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis (survey annex Q3.6).

Another objective of CE2014 relates to the efficiency of emergency responses, e.g. whether ENISA's support enabled putting in place emergency mitigation and responses at low resource and time cost. In the survey only 49% of stakeholders agreed/strongly agreed with a statement to this end (survey annex Q4.8), well below the 70% success threshold. However, it should be noted that efficiency is not an explicit objective of the cyber exercises. The case study results suggested that C2014 is working towards ensuring 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. However, the opportunity has not yet arisen to make use of EU-Standard Operating Procedures (EU-SOPs) and national capabilities need to be further built up in order to ensure the effective management of large-scale cyber incidents at the European level.

A question in the survey concerned whether technical capacity had increased among involved stakeholders, to which 42% agreed/strongly agreed (survey annex 4.7). The number of respondents is fairly low (47 persons) and several responses were neutral, making it difficult to draw any firm conclusion on the findings. The CE2014 case study did not shed much more light on this aspect, suggesting that the technical operations part of the exercise (TLEx) will have contributed to identifying gaps in technical capacity, but in a number of cases interviewees were not party to this exercise, felt that the technical teams had worked "very well", or stressed that this is a sensitive area among the private sector and that even if gaps had been identified (and later dealt with), the players would not necessarily have disclosed these and kept the lessons learned to themselves.

Concerning the sharing of lessons learned from the cyber exercises, this was positively assessed by 72% of the stakeholders, as can be seen in the figure below. There were no major differences between stakeholder groups, which indicate that the sharing of lessons learned is effectively reaching the broader community.

Figure 16 Q4.4 ENISA effectively shares lessons learned from cyber exercises with other communities and sectors



The case study conducted on CE2104 further suggests that the lessons learned from the exercises are being shared through the After Action Report and national-level post-exercise debriefing sessions, with in some instances these sessions being broadened to include people other than exercise participants. Lessons learned tend to be shared within a semi-closed circle of interested parties or disseminated to higher political levels due to the sensitivity of the information, which acts as a legitimate barrier to wider dissemination. Moreover, it was concluded as part of the case study that CE2014 facilitated the exchange of ideas, good practices and common exploration areas, and the sharing of lessons learned among communities and sectors. However, interviewees mentioned that there is a discrepancy between the exercises and real life as in real life people will favour established contacts over news ones.

Despite issues of a lack of trust and a tendency to continue contacting established contacts after an exercise has been carried out, the case study concluded that the planning and implementation of CE2014 facilitated cooperation between operational communities, and that one of CE2014's key achievements is its contribution to enhancing community building in Europe and beyond. As one interviewee put it, "even if we don't call every day, we met, exchanged things, and worked together, so CE2014 did contribute to building a community of crisis managers".

5.3.4.2 Work package 3.2 Implementation of EU legislation

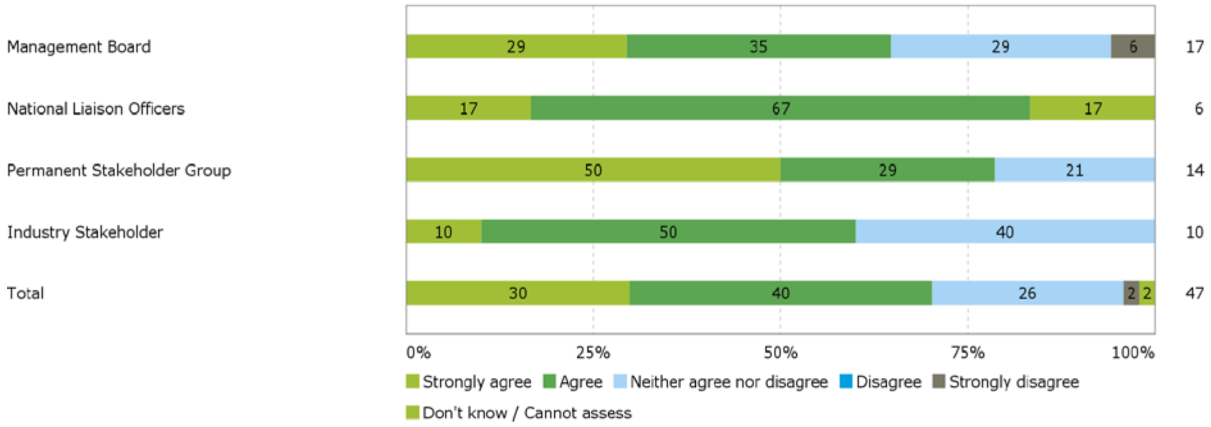
Under this work package the implementation of Article 13 (a) is followed up. The deliverable 'Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents' (D1) involved contributions from all 28 Member States and two EFTA countries who sent their annual summaries of incidents. The KII was set at 23 Member States. The technical guidelines for these reports set up by ENISA were followed. No specific survey question addressed work conducted by ENISA in the field of incident reporting. According to interviews with ENISA staff, the report collects and analyses information on incidents and pick up good examples on mitigation for dissemination. To this end ENISA provides an aggregated view and an opportunity to exchange knowledge and lessons learned on past incidents.

5.3.4.3 Work package 3.3 Regular cooperation among NIS communities

The objective of this work package was to enhance the cooperation between operational communities, such as CERTs and law enforcement agencies. Two of the deliverables under this work package were relevant for the evaluation. The 'Good governance guide and/or training and exercise material for the exchange and processing of actionable information CERTs' (D2) achieved its targets in terms of Member States supporting the good practice guide and trainings. The same goes for the 'Draft report "Stocktaking on channels and formats for exchange of operational information"' (D3).

Respondents to the survey confirm that ENISA's support has contributed to enhanced cooperation in operational communities. In the survey, 70% of the stakeholders agreed/strongly agreed, in line with the threshold set for the evaluation.

Figure 17 Q4.5 ENISA's support has contributed to enhanced cooperation in operational communities



It can be reasonably concluded that ENISA's support to enhance cooperation in operational communities has been successful. A related question concerned community building in Europe and beyond, e.g. international dimensions, where respondents were more positive with 78% agreeing/strongly agreeing (survey annex Q4.9). In open comments the respondents lifted the need to strengthen and develop relationships with senior level and decision makers at the national levels.

- *More resources needed and more attention by MS at a senior level (MB/NLO)*
- *ENISA's relationship with senior decision makers in the Member States needs to be developed. (PSG/industry)*
- *ENISA should have better instruments to help industry to come together to share experiences, best practices, projects... to build up a strong and resilient ICT sector in EU (PSG/industry)*
- *ENISA achieved excellence in creating a community of practice that links various stakeholders; its contribution here is invaluable. (PSG/industry)*

In the case study, the findings points towards that C2014 enhanced cooperation between operational communities to a relatively limited extent as this is a long-term process which involves the building of trust. During the exercises themselves, a number of actors did not cooperate with each other / across the public-private divide, few Member States involved public affairs experts, and opportunities for cooperation at multinational level were not provided. Moreover, cooperation levels with other communities post-exercise seem to remain the same – though with existing relationships having been strengthened.

Findings show that the work stream 3 has largely achieved the objectives set, with stakeholders assessing a clear contribution of ENISA to putting in place effective measures to cope with cyber crises and incidents. In particular, ENISA’s support was considered valuable to improve workflow and cooperation among involved stakeholders. In terms of regular cooperation and community building, the objectives were achieved and ENISA’s support is seen as valuable and relevant.

That said, as the CE2014 case study concludes, there is still a long road ahead before an EU-level crisis management process is put in place in the cyber security area, with a lack of trust among stakeholders, weaknesses and differences in national capabilities, weak communication structures, insufficient exchanges of information in “real life” etc., representing hurdles that need to be surmounted over the medium to long term.

5.4 Efficiency

Efficiency has been assessed based on 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.

In the interviews with staff, the cost saving measures were discussed, and according to interviewees, regular follow up on costs take place, and, in general, expenditures are comparable across projects, for example costs of use of expert group (same way of estimating costs of expert group) and alike. However, no concrete costs saving measures were identified, but it was assumed that the Agency worked as efficiently as possible.

5.4.1 Costs and resources per work stream

In the Table 5 on the next page, an overview of costs per work stream, work package and individual deliverable is presented. Based on the statistics on downloads of deliverables from the ENISA website up until end June 2015, a calculation of cost per download has been made.

Evidently, the cost per download will go down as time passes and more downloads take place. Since the current evaluation is the first in a series of yearly evaluations to be conducted, the tracking of costs per deliverable will serve as a baseline, against which subsequent years’ evaluations can follow-up on developments. It should be strongly emphasised that the tracking of costs cannot lead to judgements in itself on the cost-effectiveness of individual deliverables, since the actual impact of deliverables is not necessarily connected to a high or low cost.

The calculation for 2014 deliverables shows that there is a great deal of variance in cost per download. While this is probably mainly due to the date of publication (and hence the period of availability to download), it may also be explained by the nature of the report. For example the "Impact assessment and roadmap (CERT)" had the highest ratio in 2014 with 59.30 Euros per download, which may be linked to the fact that it is a methodological or follow-up report, rather than an operational or functional document. Another deliverable with a relatively high cost ratio per download was the "Best practice guide on exchange processing of actionable information — exercise material", again not a deliverable which is directly functional or operational, with a ratio of 23.20 Euros. On the lower end in terms of cost ratio we find deliverables such as "Minimum Security Measures for Cloud Computing" (2.41 Euros); "An evaluation framework for Cyber Security Strategies" (3.09 Euros); and "Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents" (3.61 Euros). The cost ratios appear to be more driven by number of downloads than higher/lower development costs. Looking at the average cost ratios across work streams, the differences even out with an average ratio between 5.39 to 7.89 Euros.

In terms of resources and staff, the division between work streams is fairly equal. The largest number of FTEs are allocated to work stream 3, with 14 FTE, but it should be kept in mind that the cyber exercise is a biannual event, and the number of FTE allocated in 2014 probably reflect this. It is not possible to break down FTE per deliverable.

The operational budget of ENISA is limited, and the main expenditure relates to staff costs. 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. No indication of low efficiency was identified in the evaluation period, though specific cost saving measures could not be established.

Table 4 Overview cost and staff per deliverable (source ENISA)[29]

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	60,024	13,002	4.62
		D2	Threat Landscape and good practice guide for smart home and converged media	25,000	3,705	6.75
			Threat Landscape and good practice guide for Internet infrastructures	24,588	4,308	5.71
	WPK1.2 Contributing to EU policy initiatives	D3	Algorithms, key size and parameters report 2014/Study on cryptographic protocols	72,472	16,706	4.34
	WPK1.3 Supporting the EU in education, research and standardisation	D1	Standardisation in the field of Electronic Identities and Trust Service Providers	30,288	1,695	17.87
Total WS1				**212,372**	**39,416**	**5.39**
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	39,386	12,747	3.09
		D6	Impact assessment and roadmap (CERT)	80,476	1,357	59.30
	WPK 2.2 Support Private Sector Capacity Building	D2	Smart grid security certification in Europe;	42,450	2,641	16.07
		D3	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts;	48,528	3,799	12.77
		D5	Minimum Security Measures for Cloud Computing (two reports)	37,722	15,666	2.41
		D7	Methodologies for the identification of critical information infrastructure assets and services	33,618	2,477	13.57
		D8	Network and Information Security in the Finance Sector — Regulatory landscape and Industry priorities	49,282	4,286	11.50
Total WS2				**331,462**	**42,973**	**7.71**
WS3 - Support Cooperation Staff resources FTE 14.0	WPK 3.1 Crisis cooperation - exercises	D1	Cyber Europe 2014: Exercise Plan and Exercise	127,944	1,400 Participants	91.39 (per participant)
			Report on Cyber Crisis Cooperation and Management	30,138	2,269	13.28
	WPK 3.2 Implementation of EU legislation	D1	Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents	62,132	17,198	3.61
	WPK 3.3 Regular cooperation among NIS communities	D2	Best practice guide on exchange processing of actionable information — exercise material	93,000	4,016	23.16
Total WS3				**185,270**	**23,483**	**7.89**

[29] The overview does not contain all activities of under the WP 2014. Only deliverables with a publication and their associated cost have been included, plus the CE 2014.

5.5 Coordination and coherence

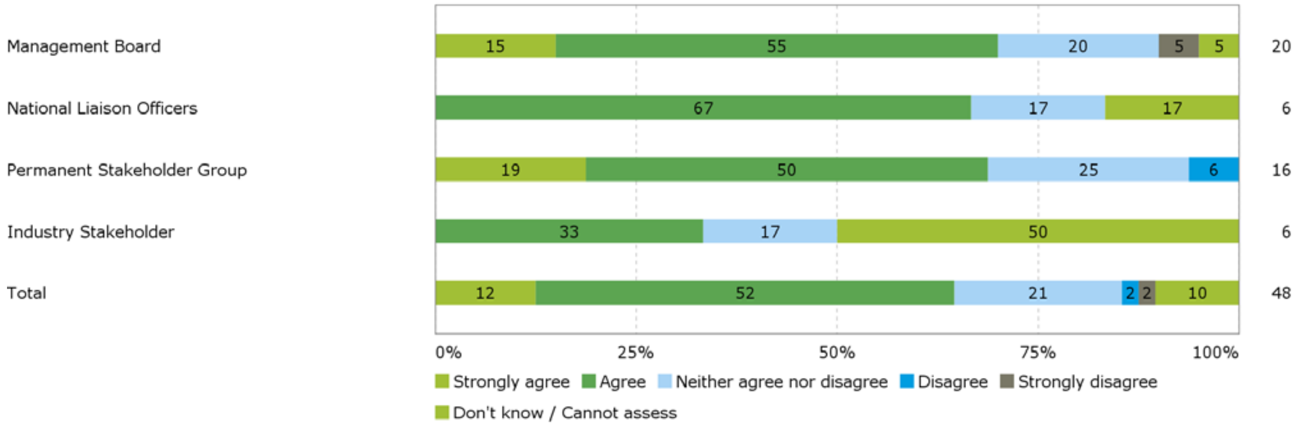
An important aspect of ENISAs' work is the coordination and cooperation with involved stakeholders in NIS at the EU, Member State and international level. In interviews with staff, it was generally believed that the main stakeholders were sufficiently involved and consulted. Indeed, it was stressed that this is the only way ENISA can function, as it does not have the resources or mandate to carry out work differently. In terms of different stakeholder groups, interviewees mentioned that the private sector sometimes was difficult to engage, since ENISA is not a regulatory body and/or that no funding for participation can be provided.

According to interviews with ENISA staff, there is no real alternative or similar body to ENISA at international level, even though the OECD carries out some similar work as well as sectorial organisations/associations. At national level in Member States there are public bodies with a similar scope of work, but at the EU level ENISA holds a unique position.

Coherence concerns to what extent ENISA's activities complement other initiatives in the same or similar field. In the survey to stakeholders this was supported by the respondents in relation to work stream 1 support to EU policy and to work stream 3 support to cooperation (well above 70% agreed/strongly agreed, survey annex Q2.3 and Q4.3).

Respondents were less certain that the support provided by ENISA in capacity building complemented that of other public interventions, with 64% agreeing/strongly agreeing. However, since the number of people responding to this question was low, it is difficult to draw any firm conclusion on the answers.

Figure 18 Q3.3 The support provided by ENISA in capacity building complements that of other public interventions



Finally, CE2014 was found by interviewees to complement other public (and private) interventions, such as national level cyber exercises which are situated at a different level and have a different focus to CE2014, or the Integrated Political Crisis Response Arrangements (IPCR) exercise at EU level which was a spin-off of CE2014 (see case study). In fact, one interviewee stressed the importance of having such exercises at EU level as this meant that private companies had to act as international stakeholders, which would not be possible at national level.

Overall, it can be concluded that ENISA's effectively cooperates and engages with its main stakeholders as stipulated in the mandate. The support provided by ENISA is seen as a complement to that of other public interventions, and no adverse effects were identified.

6. CONCLUSIONS AND RECOMMENDATIONS

The following section presents the overall conclusions of the evaluation related to the evaluation criteria and evaluation questions. The conclusions are based on the findings presented in the earlier chapters. Following on from the conclusions, recommendations for improvement are presented where pertinent.

6.1 Relevance

The core operational activities carried out under the Work Programme 2014 have a clear connection to the legal mandate of ENISA. There were no instances of activities falling outside of the mandate identified and thus it can be concluded that ENISA carried out its activities as foreseen in the regulation.

The evaluation findings also show that ENISA clearly responds to a need in the European NIS landscape; a conclusion which is supported by the 2011 study conducted by the European Parliament on "The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally" which acknowledged that ENISA's function was, at the time, increasingly seen as valuable and necessary, and that its effective mission had steadily grown over the years.

The scope and objectives of ENISA's work is seen as relevant to respond to the needs, but at the same time stakeholders see limits in ENISA's mandate and outreach. In particular, private stakeholders and industry appear to strive towards a more operational role for ENISA, going beyond the advisory and facilitating mandate of the Agency, in order to effectively achieve the overall objectives of NIS and cyber security. Such views were also expressed in the European Parliament's study, where experts noted that in the future ENISA might consider taking a limited operational role in combating cyber threats (e.g. taking on 24 x 7 responsibilities), instead of just facilitating these activities. However, this wish or demand is not echoed by Member States and it does not seem likely that ENISA's mandate will be broadened in the near future.

There are no detailed recommendations to be distilled from the evaluation in relation to relevance, but it can be noted that ENISA carries out a high number of core operational activities (in light of limited resources). A recurring comment from stakeholders was that ENISA's ambitious objectives were difficult to achieve given the small size of the agency. This was echoed in Ramboll Management Consulting and Euréval's 2009 evaluation of 26 decentralised EU agencies which noted that the small size of ENISA makes it questionable whether it has the critical mass to produce impacts in a meaningful way or whether ENISA's "good quality products" could achieve the expected results. It may be important in the future to focus on activities where there is a strong demand from the NIS communities to ensure that ENISA's deliverables achieve a real impact.

6.2 Effectiveness

Overall, the evaluation findings are positive and on most indicators ENISA's Work Programme 2014 has achieved the intended outcomes, results and impacts, as per the judgment norm agreed for the evaluation. There is a clear pattern in terms of progress, where targets under ENISA's control (such a high quality, community building, good practice dissemination) are largely achieved. The progress towards more long term objectives looks more uncertain (preparedness to respond to crisis, increase in capacity etc.), as this is highly dependent on contextual factors as well as public and private stakeholders' engagement and investment. Still, a majority of consulted stakeholders were of the opinion that ENISA clearly contributes to ensuring a high level NIS in the EU, which should be seen as a strong achievement.

In terms of organisation and ENISA's internal functioning, the Agency seems to be largely well functioning. There are current and forecasted issues with staff shortages and difficulties in recruiting, which according to interviews could have an impact on the Agency's capacity going forward. In order to maintain a high level of expertise, the Agency must be able to attract and retain the right people, and this is currently proving difficult. There were few indications in the evaluation that ENISA did not have the right competences or sufficient capacity during 2014, but this should be followed up carefully in coming evaluations.

The division of the Agency between Heraklion and Athens sometimes leads to cumbersome work processes and lack of communication and cooperation, but it seems like ENISA staff and managements have found ways to cope with the situation and minimise negative impact. While it would certainly be more effective and efficient to have only one location, it does not look feasible in the foreseeable future. It should be noted that the evaluators did not visit Heraklion for the current evaluation; this should be taken into account when planning for the evaluation of 2015 core operational activities.

Project management and work processes are well in place, although the project management tool Matrix does not serve the purpose of day to day management. Initiatives were under way during the evaluation period to implement common "spread sheet" models across departments for day to day management of projects, this would be a good development.

Overall, the effectiveness of ENISA's activities in 2014 is assessed as good. A general observation can be made regarding the broad scope of the activities and high number of deliverables in 2014. In light of limited resources and the inherent difficulty reaching more long term impact, it could be considered to narrow the scope and number of activities, and to concentrate efforts in order to maximise chances of reaching impact. In the current evaluation the findings did not provide any direction in particular as to what activities were most effective. However, in the evaluators' opinion the findings are not sufficiently robust to draw firm conclusions, due to the limited stakeholder group consulted. This should be addressed in subsequent evaluations.

6.3 Efficiency

The operational budget of ENISA is limited, and the main expenditure relates to staff costs. 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. No indication of low efficiency was identified in the evaluation period, though specific cost saving measures could not be established.

The tasks of the ENISA and the physical location of the Agency require extensive travel by all operational staff. A more central location (in Europe) of the Agency would have been more efficient and could save travel expenses and staff resources. While relocation is not feasible under the current mandate, it should be considered when reviewing ENISA's mandate in 2018.

It should be noted that efficiency is difficult to assess without a baseline or comparison to relate to. In future evaluations, tracking of costs over years will be conducted. It could also be envisaged to compare ENISA's costs to other (comparable) EU Agencies, on indicators such as administrative costs, travel costs, etc.

6.4 Coordination and coherence

Overall, it can be concluded that ENISA's effectively cooperates and engages with its main stakeholders as stipulated in its mandate. The support provided by ENISA is seen as a complement to that of other public interventions, and no adverse effects were identified.

No specific recommendations can be deduced from the findings relating to coordination and coherence.

7. ACTION PLAN

The following table summarises the findings per evaluation criteria and outlines tentative actions for ENISA to consider. As the evaluation of 2014 core operational activities is largely positive, the actions mainly relates to a continuation of the work carried out.

Criteria	Summary findings	Possible Actions
Relevance	Based on the findings, it can be concluded that ENISA clearly responds to a need in the European NIS landscape. The scope and objectives of ENISA's work are seen as relevant to respond to the needs, but at the same time stakeholders see limits to ENISA's mandate and outreach, which affects the ability of the Agency to effectively meet the needs.	Continue to explore ways to ensure ENISA's work is addressing real needs in NIS in the EU. Map/assess gaps in current NIS landscape, to feed into discussions on future mandate. It may be important in the future to focus on activities where there is a strong demand from the NIS communities to ensure that ENISA's deliverables achieve a real impact.
Impact	It appears that, despite ENISA's limited mandate and also fairly small resources, the Agency manages to make a real contribution towards increased NIS in Europe, as perceived by key stakeholders.	N/A
Effectiveness - KIIs and downloads	All KIIs were achieved. The evaluation can conclude that some of ENISA's deliverables have generated a high number of downloads in a short period of time (most reports were made available in Q1 2015 and thus downloads had only been available for a few months at the time of writing).	Introduce more ambitious KIIS which enable a tracking of performance.
Effectiveness - EU Policy	The evaluation findings show that the work conducted under work stream 1 has been successful in achieving most objectives. In particular the work undertaken to identify evolving threats, risks and challenges, and the contribution to EU policy initiatives appear to have achieved the intended results. For the work done in supporting the EU in education, research and standardisation, results were more mixed, in particular regarding the link to actual operational issues such as data protection and secure services. These aspects are evidently not under the direct control of ENISA but of national regulators and operators, hence the need for further efforts in coordination and cooperation.	Continue efforts to build relations with senior decisions makers at Member State and EU level (public and private).
Effectiveness - Capacity building	ENISA's work to develop capacity in Member States (to coordinate and cooperate during crises, and the support to develop capacities and strategies at Member State level) as part of work stream two has been successful in achieving the objectives set out. The	Continue to engage with the private sector to improve and increase outreach.

	contribution to private sector capacities looks more uncertain, based on the responses from the stakeholder survey.	
Effectiveness - Support cooperation	Findings show that the work stream 3 has largely achieved the objectives set, with stakeholders assessing a clear contribution of ENISA to putting in place effective measures to cope with cyber crises and incidents. In particular, ENISA's support was considered valuable to improve workflow and cooperation among involved stakeholders. That said, as the CE2014 case study concludes, there is still a long road ahead before an EU-level crisis management process is put in place in the cyber security area, with a lack of trust among stakeholders, weaknesses and differences in national capabilities, weak communication structures, insufficient exchanges of information in "real life" etc., representing hurdles that need to be surmounted over the medium to long term.	Continue trust building and cooperation activities as a means to overcome barriers to cooperation during crisis.
Efficiency	The operational budget of ENISA is limited, and the main expenditure relates to staff costs. 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. No indication of low efficiency was identified in the evaluation period, though specific cost saving measures could not be established.	N/A
Coordination and coherence	Overall, it can be concluded that ENISA effectively cooperates and engages with its main stakeholders, as stipulated in its mandate. The support provided by ENISA is seen as a complement to that of other public interventions, and no adverse effects were identified.	N/A

ANNEXES

ANNEX A: SURVEY RESULTS

1. RELEVANCE OF ENISA'S WORK 1

1.1 The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the Member States 1

1.2 The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the EU 1

1.3 The outputs produced by ENISA are responding to the needs for NIS in the Member States 1

1.4 The outputs produced by ENISA are responding to the needs for NIS in the EU 2

1.5 Please provide additional comments as relevant 2

1.6 ENISA is effectively meeting stakeholder expectations 2

1.7 It is clear what ENISA expects from stakeholders 3

1.8 Please provide additional comments as relevant: 3

2. WORKSTREAM 1: SUPPORT TO EU POLICY 4

2.1 Are you familiar with ENISA support to EU Policy? 4

2.2 ENISA's deliverables about NIS threats in the EU are relevant and of high quality 4

2.3 ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions 4

2.4 The input provided by ENISA to develop new policies for NIS in the EU is useful 5

2.5 The input provided by ENISA to implement new policies for NIS in the EU is useful 5

2.6 ENISA provides stakeholders with relevant information on standardisation, innovation and research 5

2.7 ENISA's outputs and deliverables contribute to putting in place more effective risk mitigation strategies 6

2.8 ENISA's outputs and deliverables contribute to ensuring personal data protection and secure services 6

2.9 ENISA's outputs and deliverables contribute to setting standards for NIS and privacy 6

2.10 Please provide additional comments as relevant: 7

3. WORKSTREAM 2: SUPPORT TO CAPACITY BUILDING 7

3.1 Are you familiar with ENISA's support to capacity building? 7

3.2 Good practices in NIS have been disseminated by ENISA 7

3.3 ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States 8

3.4 ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or incidents 8

3.5 The support provided by ENISA in capacity building complements that of other public interventions 8

3.6 ENISA's support has enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis 9

3.7 Sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA 9

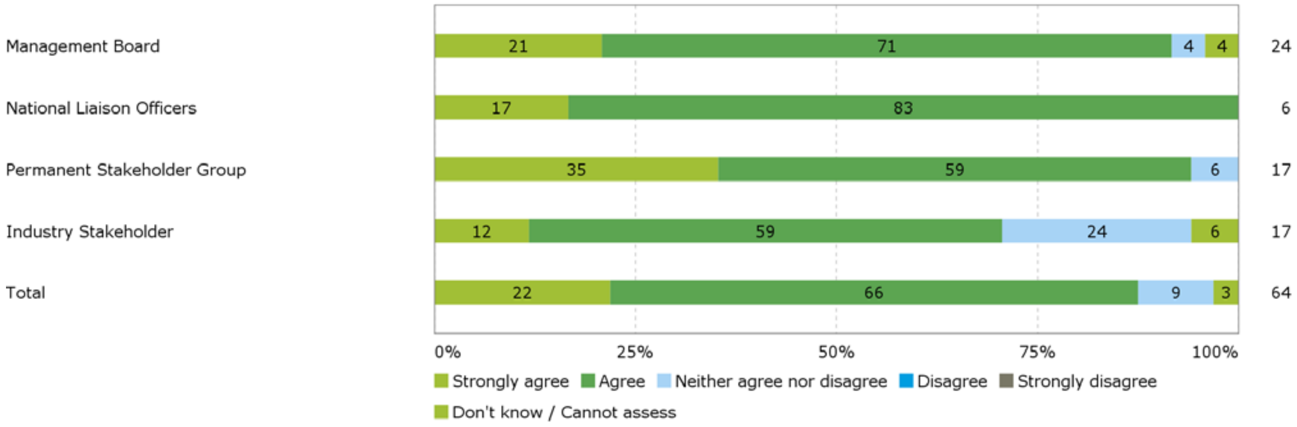
3.8 Cyber security challenges are adequately addressed in the EU 9

3.9 Cyber security challenges are adequately addressed in the Member States 10
3.10 Please provide additional comments as relevant: 10
4. WORKSTREAM 3: SUPPORT COOPERATION 11
4.1 Are you familiar with ENISA’s support to cooperation? 11
4.2 ENISA effectively supports the sharing of information, ideas and common areas of interest among stakeholders 11
4.3 ENISA’s support to cooperation between stakeholders complements other public interventions 11
4.4 ENISA effectively shares lessons learned from cyber exercises with other communities and sectors 12
4.5 ENISA’s support has contributed to enhanced cooperation in operational communities 12
4.6 ENISA’s support has improved services, workflow and communication among stakeholders to respond to crises 12
4.7 Technical capacity has increased among involved stakeholders 13
4.8 ENISA’s support has enabled emergency mitigation and responses to be put in place at low resource and time costs 13
4.9 The support from ENISA has contributed to enhancing community building in Europe and beyond 13
4.10 Please provide additional comments as relevant: 14
5. IMPACT OF ENISA’S SUPPORT 15
5.1 ENISA clearly contributes to ensuring a high level of NIS within the EU 15
5.2 ENISA clearly contributes to raising awareness on NIS within the EU 15
5.3 ENISA clearly contributes to promoting a culture of NIS in society 15
5.4 Please provide additional comments as relevant: 16
1. DO YOU HAVE ANY PARTICULAR SUGGESTIONS AS TO HOW ENISA COULD IMPROVE IN THE FUTURE? 17

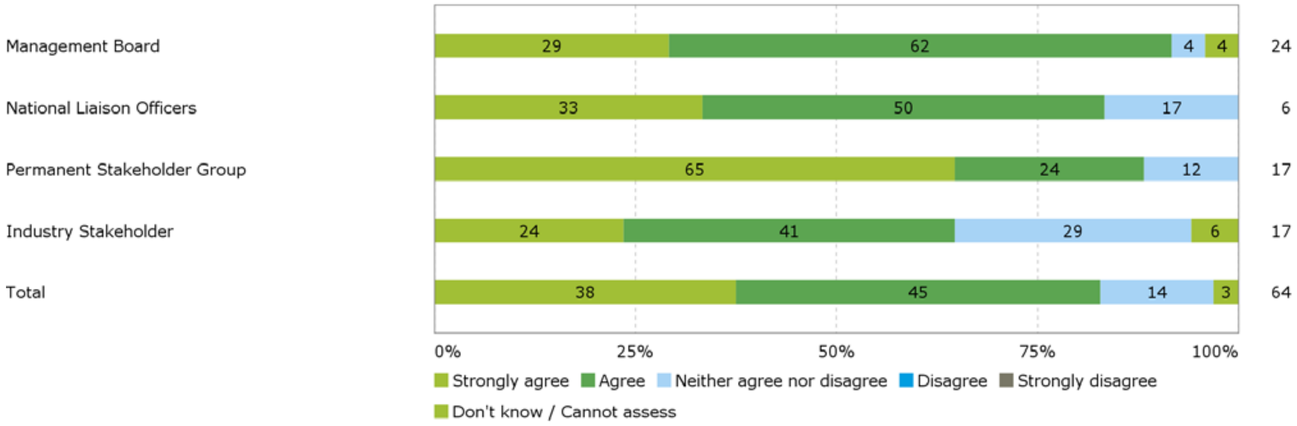
1. RELEVANCE OF ENISA'S WORK

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)

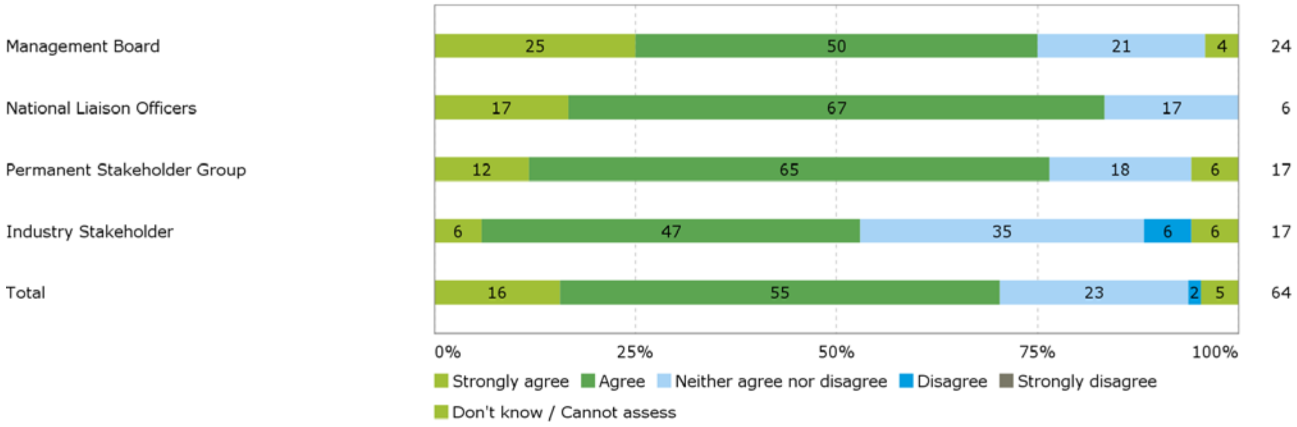
1.1 The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the Member States



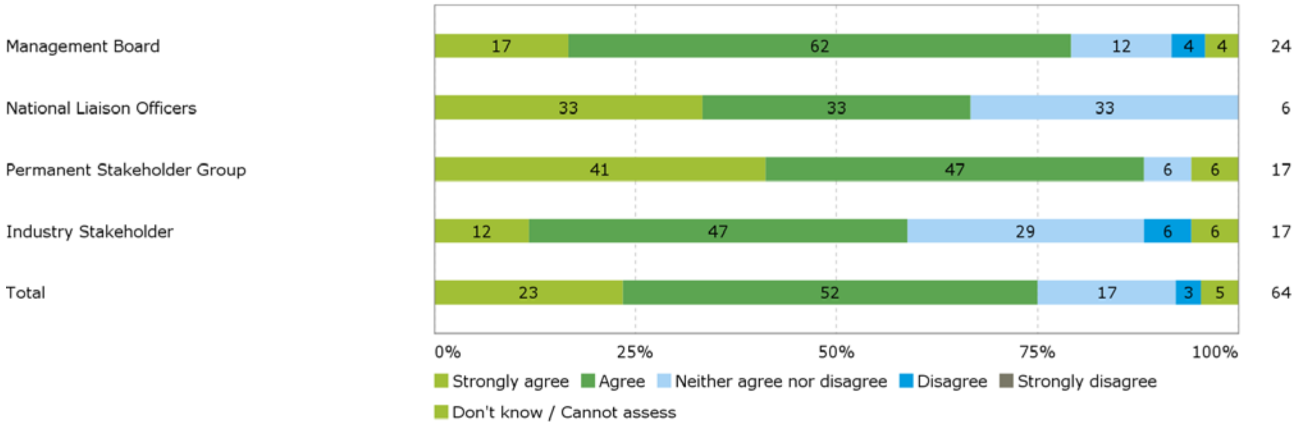
1.2 The scope and objectives of ENISA's work are relevant to responding to the needs for NIS in the EU



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



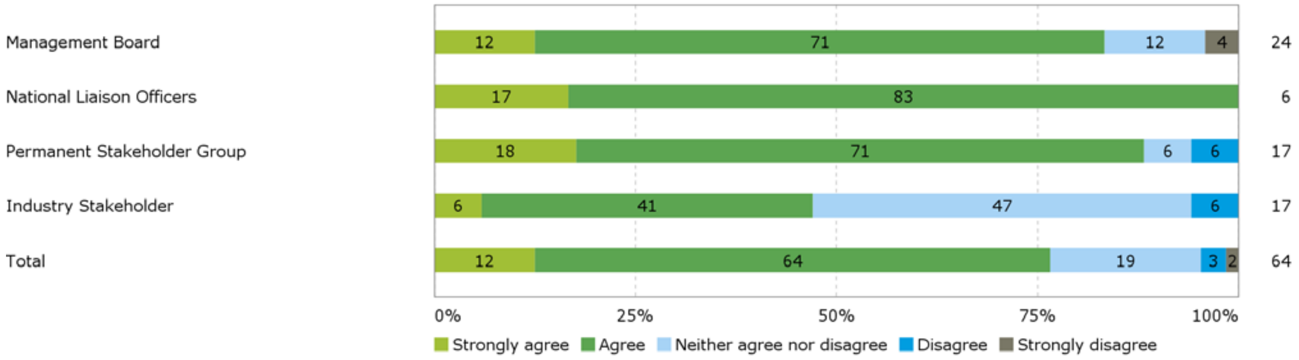
1.4 The outputs produced by ENISA are responding to the needs for NIS in the EU



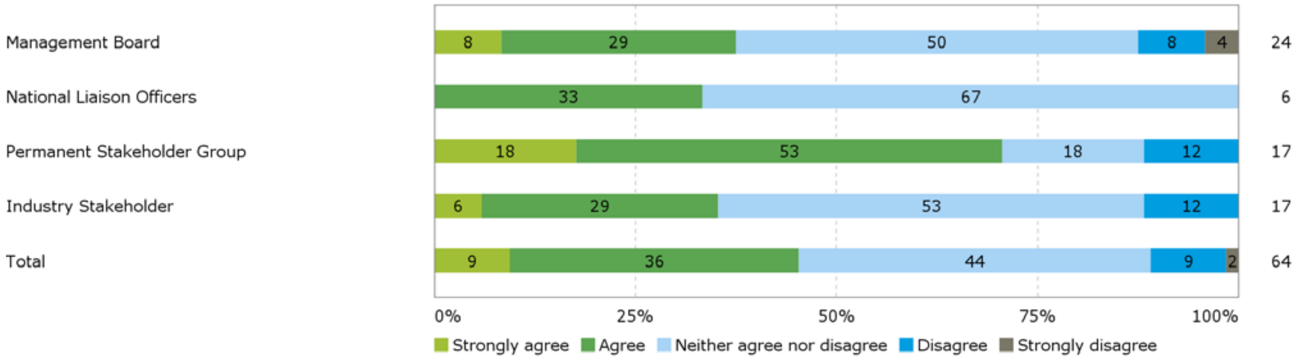
1.5 Please provide additional comments as relevant

Management Board / National Liaison Officers	Permanent Stakeholder Group / Industry stakeholders
• We believe that ENISA is responding very well to the needs of MS and the EU. However, we feel that it would be a good idea for ENISA to also take on a more operational role in terms of facilitating/coordinating the efforts of member states for the prevention and mitigation of large scale cyber attacks. • Resource limitations and restrictions in the mandate reduce the effectiveness of what could be achieved	• ENISA has been ineffective in influencing key stakeholders in and effective engagement with my Member State. • ENISA has to play a more important role, not only as a support if EU wants to play a strong position in ICT. • The output and services from ENISA is not utilised in full extend in my member state. Too low knowledge and awareness about ENISA. • I think the ENISA work is very relevant at EU level. I also think that the ENISA work is relevant at member states level but could be even more relevant if there was political will from the member states • The rating of the outputs was done considering the (still too small) budget. With more resources more would be possible.

1.6 ENISA is effectively meeting stakeholder expectations



1.7 It is clear what ENISA expects from stakeholders

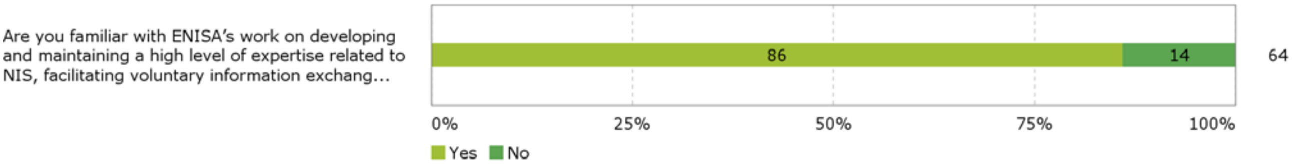


1.8 Please provide additional comments as relevant:

Management Board / National Liaison Officers	Permanent Stakeholder Group / Industry stakeholders
• See previous comment	• ENISA should support the development of ICT sector in Europe • I can't really rate this based on my knowledge about stakeholders. • Information security has a lot of stakeholders. I think ENISA is challenged to reach all of them and it is difficult to meet their expectations • ENISA could better meet expectations if it would be allowed to have a wider role • Many stakeholders would be open to greater participation in the areas of their expertise if it is congruent with ENISA's charter.

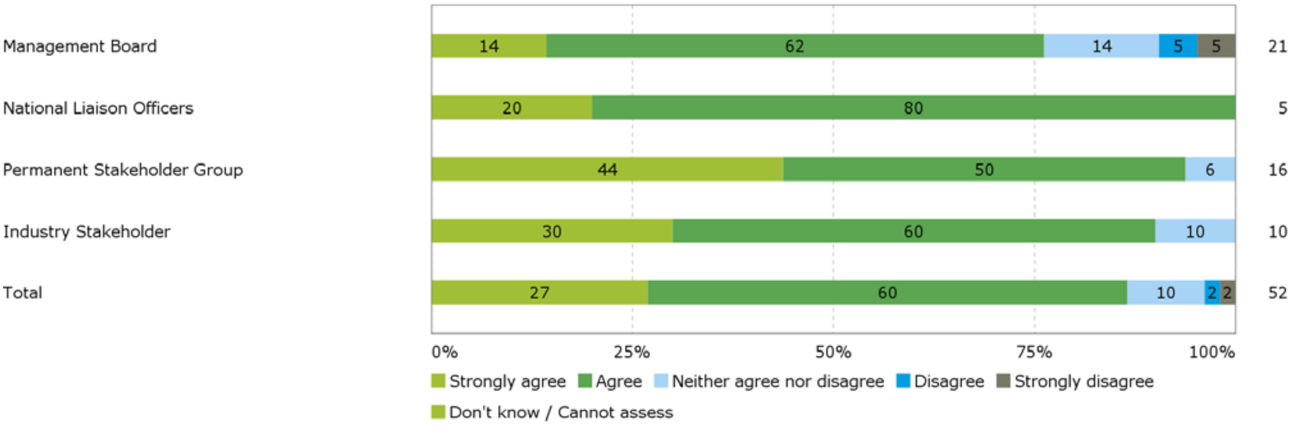
2. WORKSTREAM 1: SUPPORT TO EU POLICY

2.1 Are you familiar with ENISA support to EU Policy?

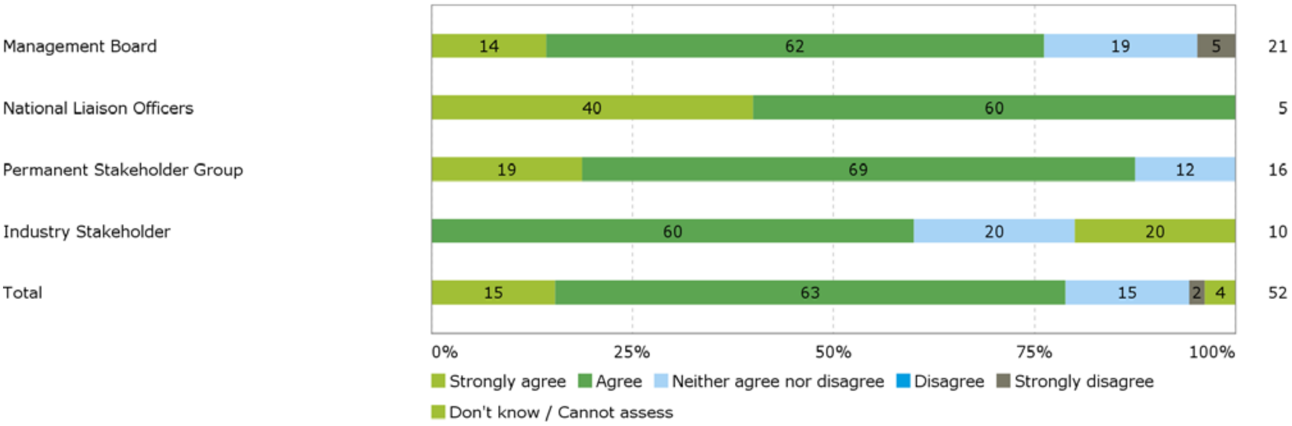


Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to EU Policy in NIS:

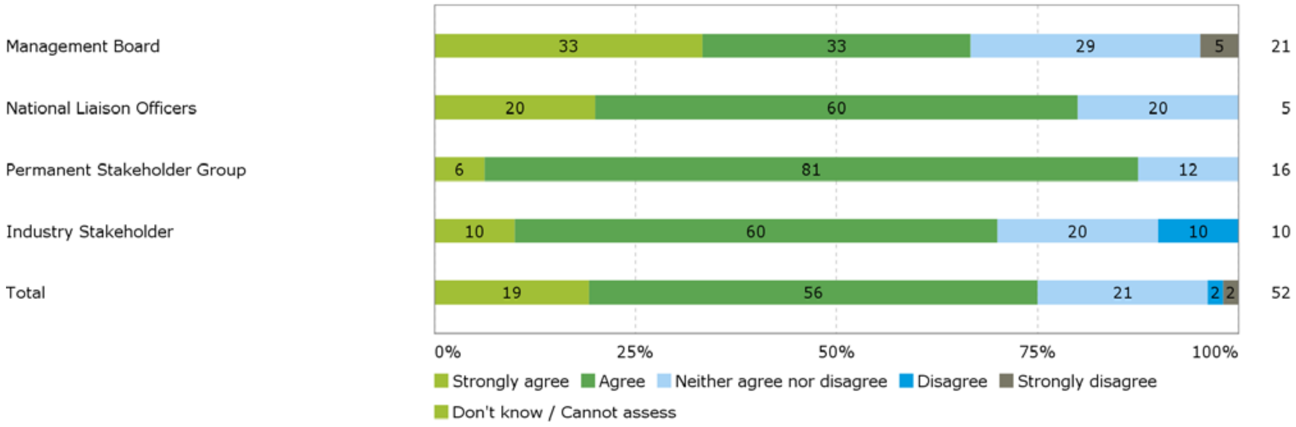
2.2 ENISA's deliverables about NIS threats in the EU are relevant and of high quality



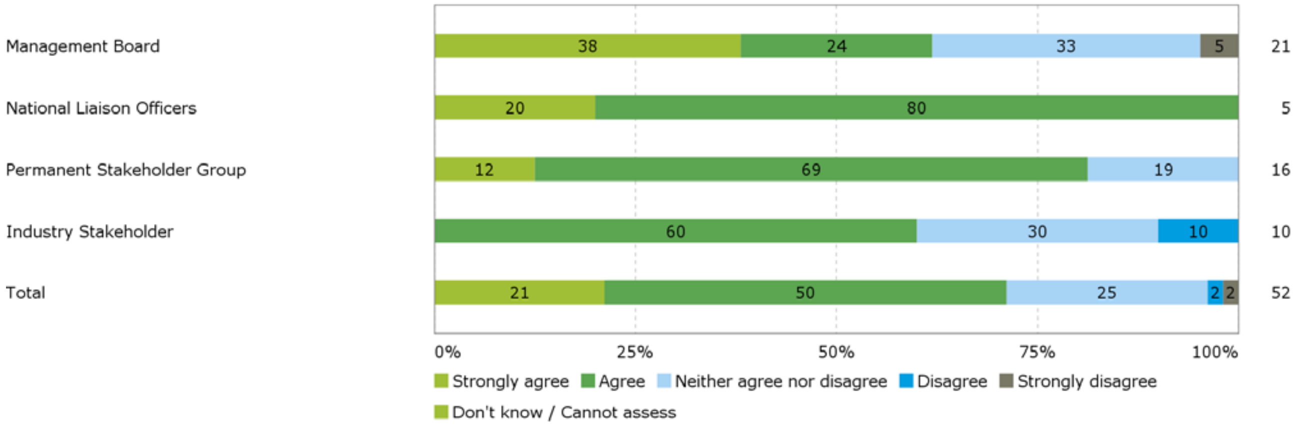
2.3 ENISA's deliverables to support NIS policy at the EU level complement those of other public interventions



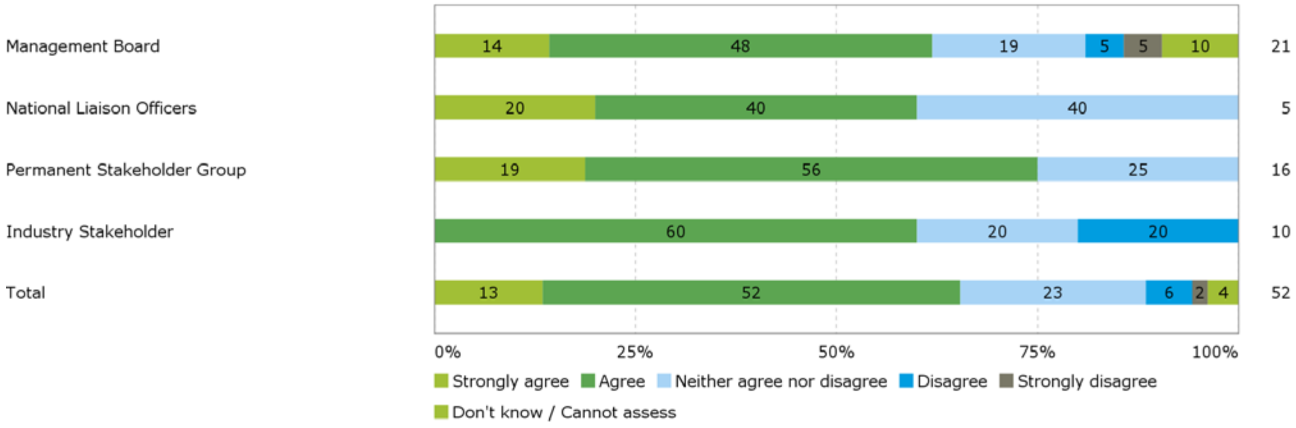
2.4 The input provided by ENISA to develop new policies for NIS in the EU is useful



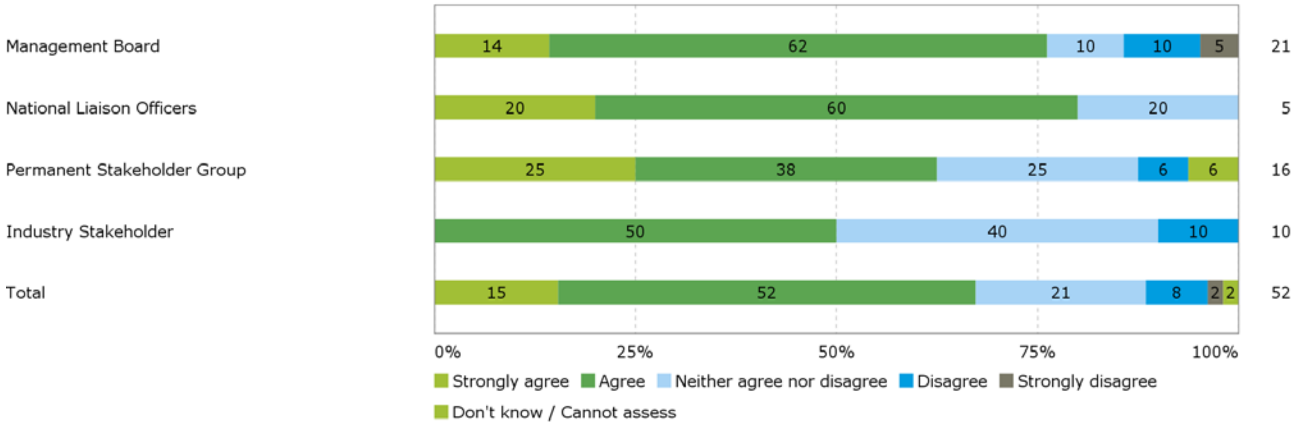
2.5 The input provided by ENISA to implement new policies for NIS in the EU is useful



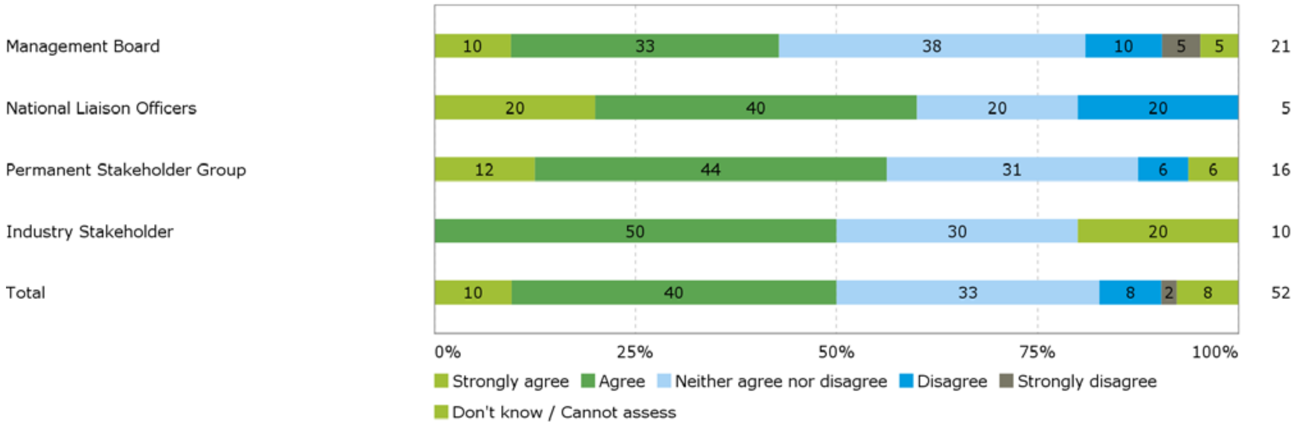
2.6 ENISA provides stakeholders with relevant information on standardisation, innovation and research



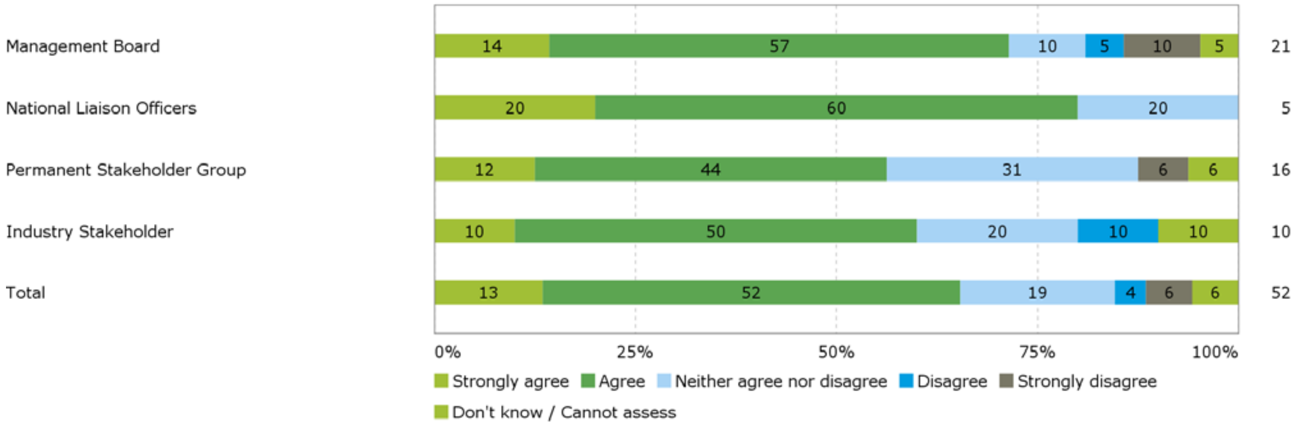
2.7 ENISA's outputs and deliverables contribute to putting in place more effective risk mitigation strategies



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

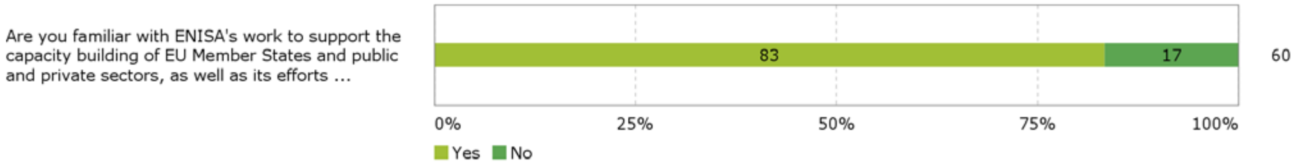


2.10 Please provide additional comments as relevant:

Management Board / National Liaison Officers	Permanent Stakeholder Group / Industry stakeholders
• NISA's work at EU level needs further effort and coordination • ENISA should be focused on building capacity and capability in the EU, rather than providing deliverables about NIS threats. The Commission should consult ENISA more thoroughly before making announcements about NIS policy (e.g. the PPP announced in the DSM communication).	• I do not see ENISA helping Members to develop its policies • Still a lot of work in progress but ENISA should remain the reference within the EU

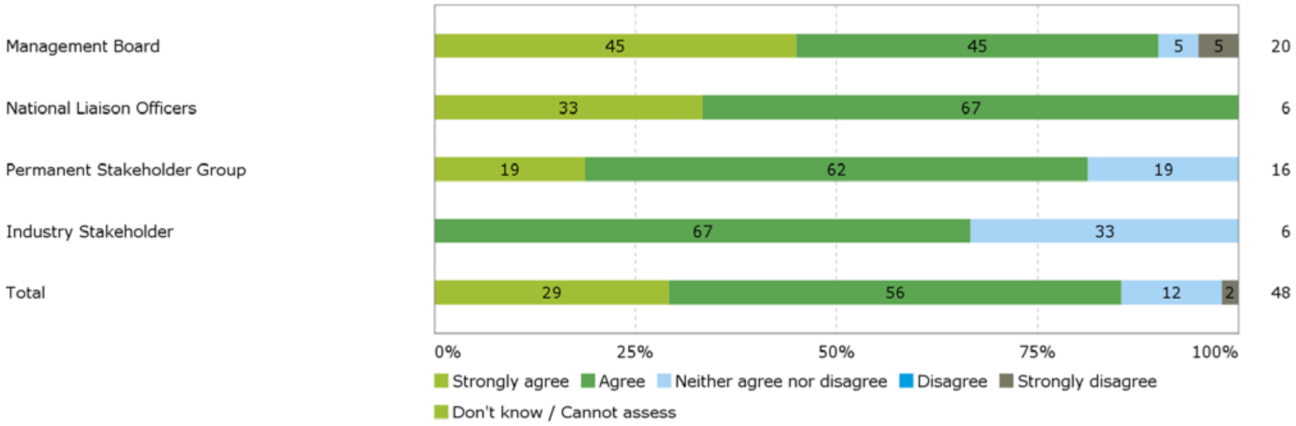
3. WORKSTREAM 2: SUPPORT TO CAPACITY BUILDING

3.1 Are you familiar with ENISA's support to capacity building?

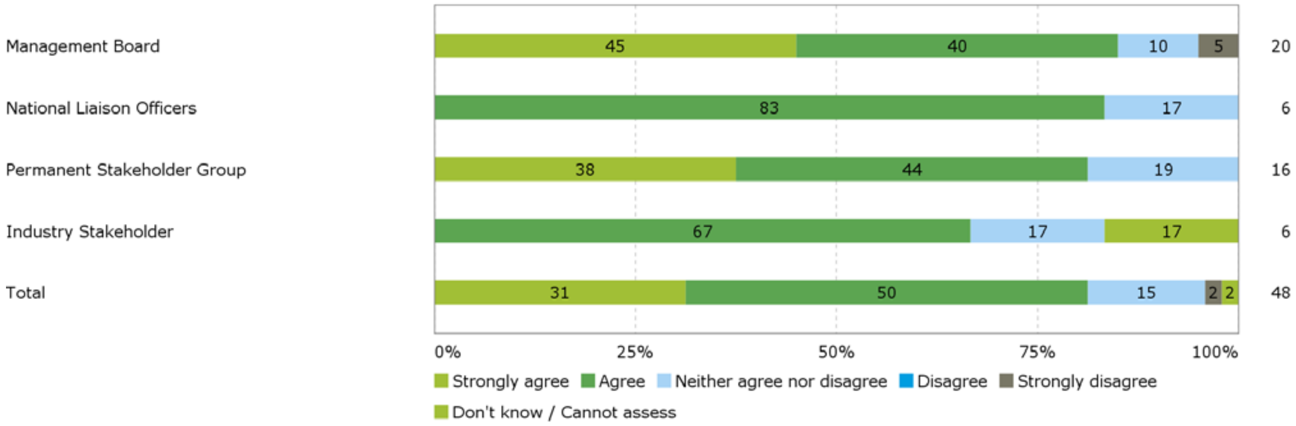


Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to capacity building:

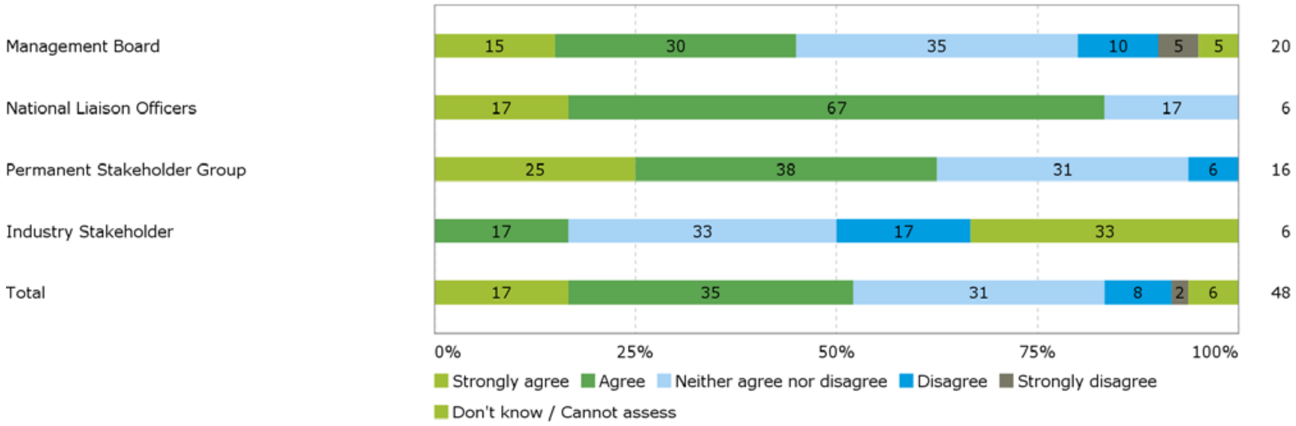
3.2 Good practices in NIS have been disseminated by ENISA



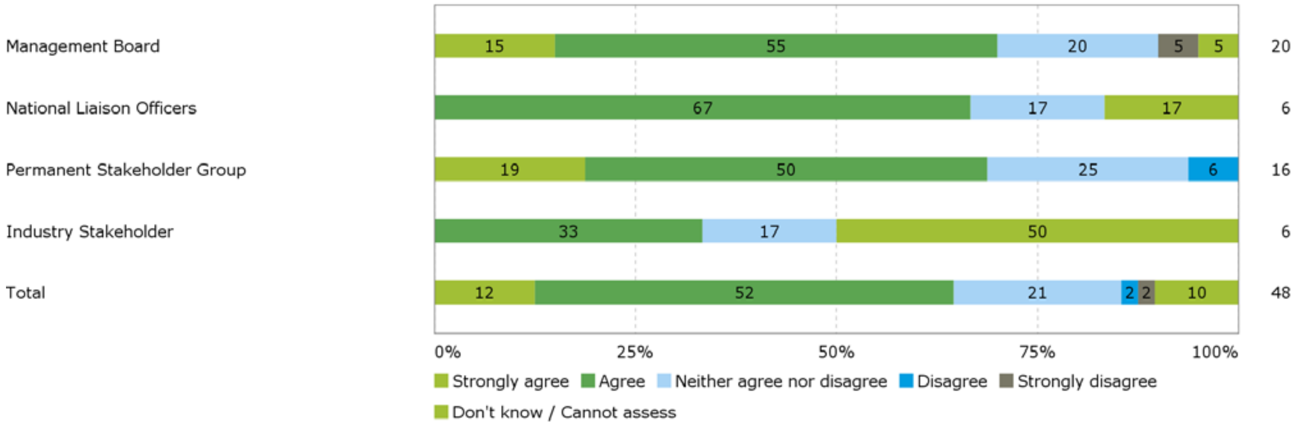
3.3 ENISA has contributed to developing capacities in prevention, detection, analysis and response in Member States



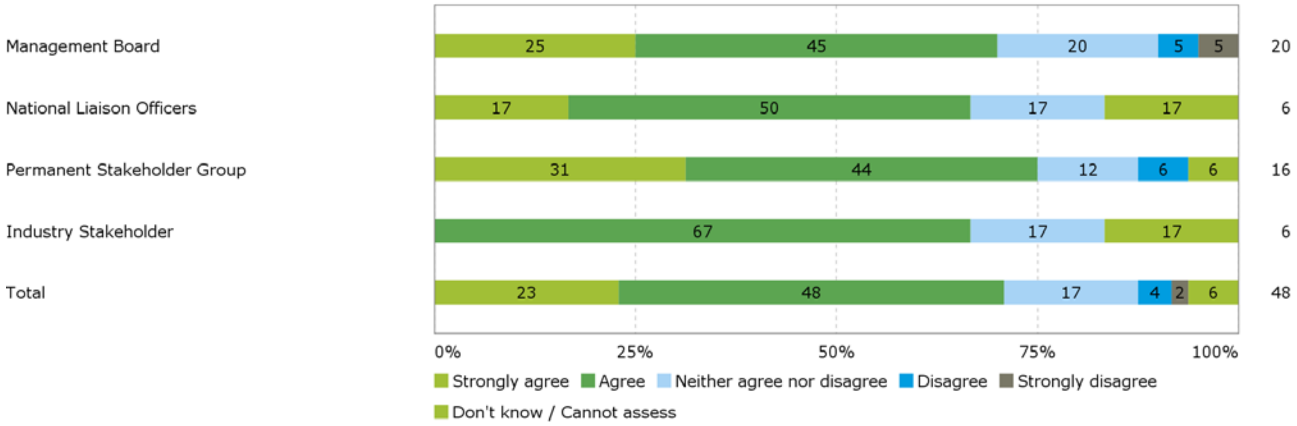
3.4 ENISA has contributed to improving the preparedness of the private sector to respond to NIS threats or incidents



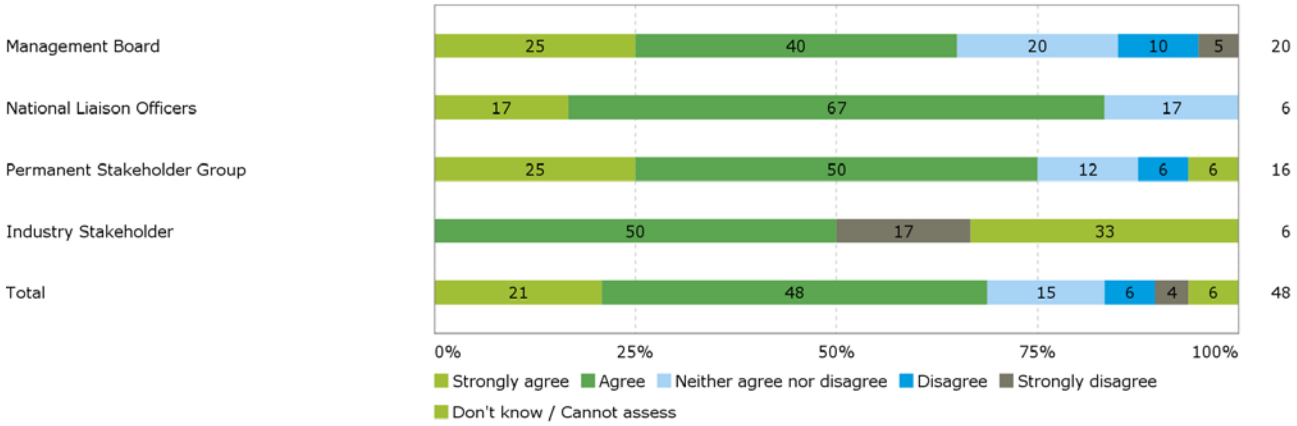
3.5 The support provided by ENISA in capacity building complements that of other public interventions



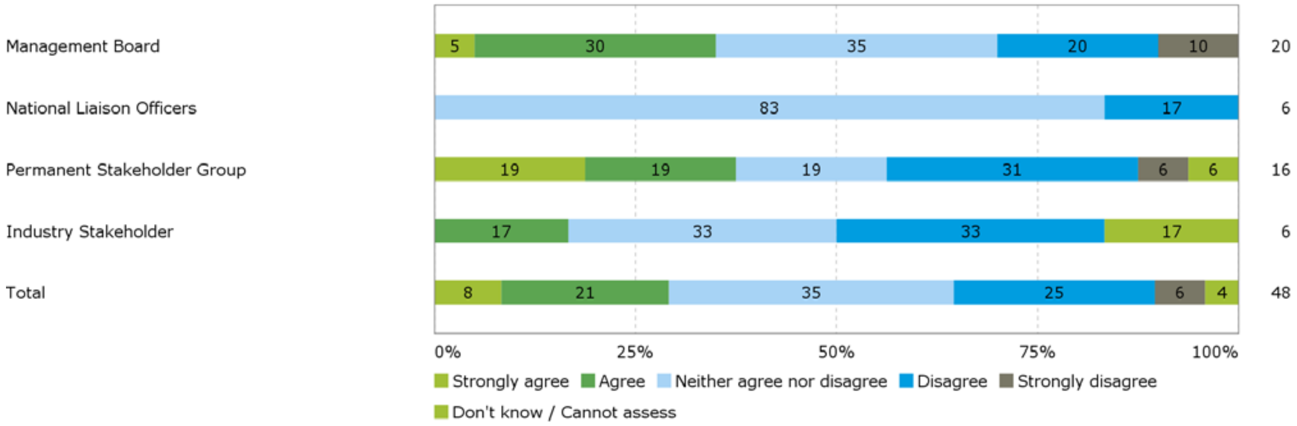
3.6 ENISA’s support has enabled relevant stakeholders to be prepared to coordinate and cooperate during a cyber-crisis



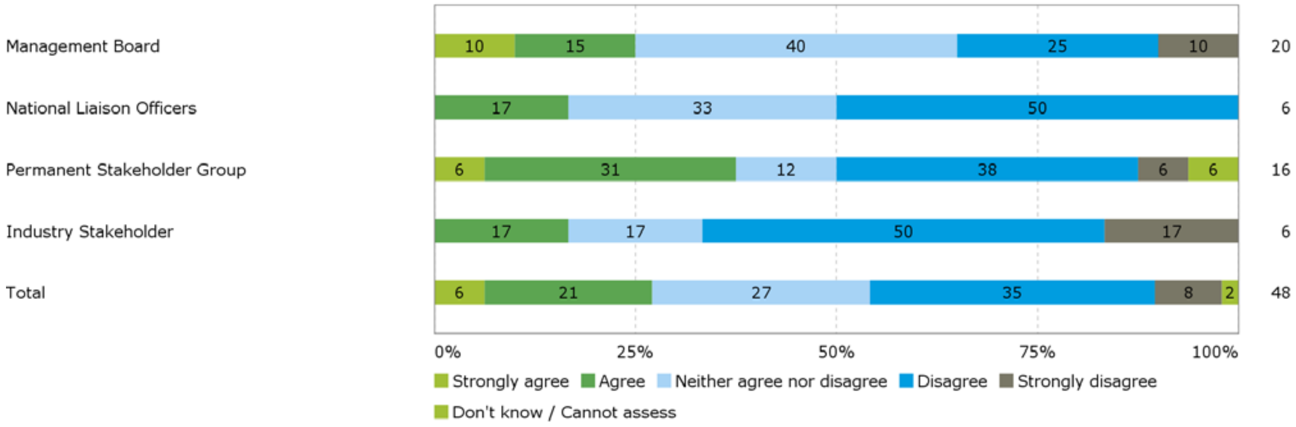
3.7 Sound and implementable strategies to ensure preparedness, response and recovery have been developed with the support of ENISA



3.8 Cyber security challenges are adequately addressed in the EU



3.9 Cyber security challenges are adequately addressed in the Member States

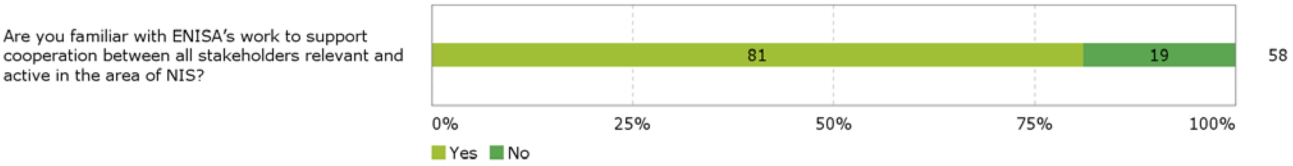


3.10 Please provide additional comments as relevant:

Management Board / National Liaison Officers	Permanent Stakeholder Group / Industry stakeholders
• Still a long way to go • ENISA should ensure that MS feedback on the Cyber Europe exercise is used to inform and improve future exercises.	• Private Sector stakeholders in my MS, dominated by SMEs, are largely ignorant of ENISA and the good practice recommendations. Direct EU outreach arrangements would be more effective. • Knowledge about ENISA is too low in private sector. Parts of public sector (national CERT, Telecom). There is a need for a more clear (communicated) cyber security strategy and roadmap on both EU and member state level. If there are strategies, they have to be communicated more.

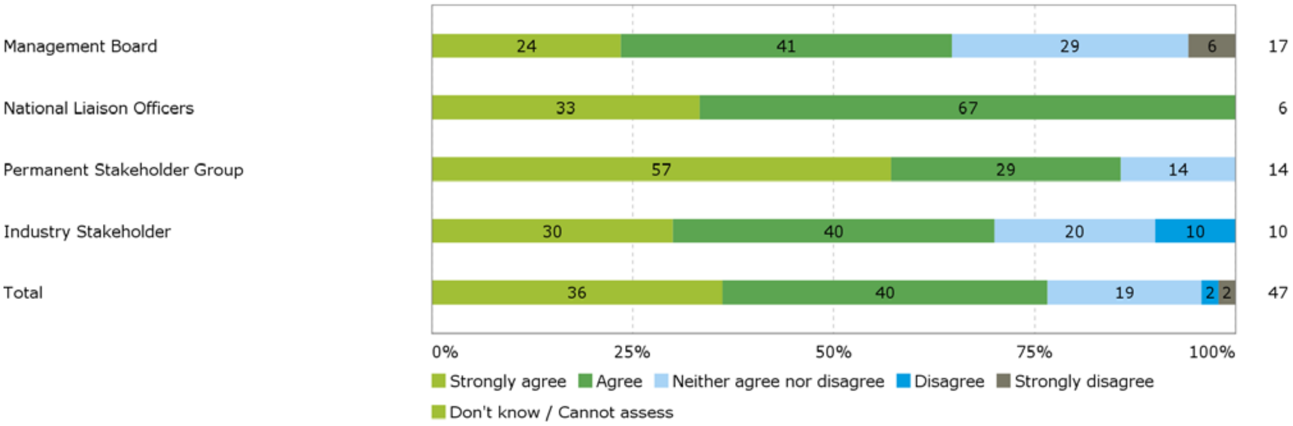
4. WORKSTREAM 3: SUPPORT COOPERATION

4.1 Are you familiar with ENISA's support to cooperation?

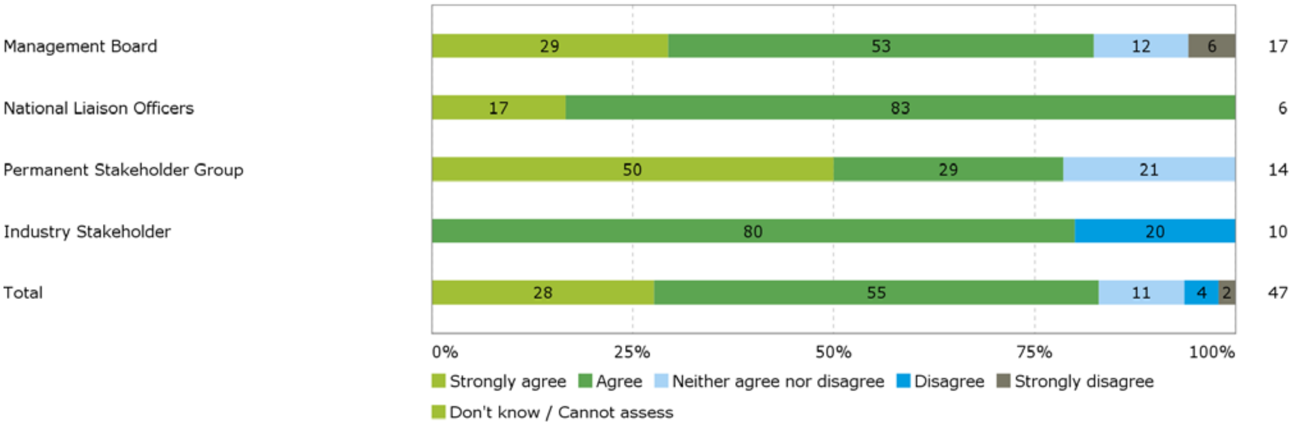


Please rate the extent to which you agree or disagree with the following statements concerning ENISA's support to cooperation:

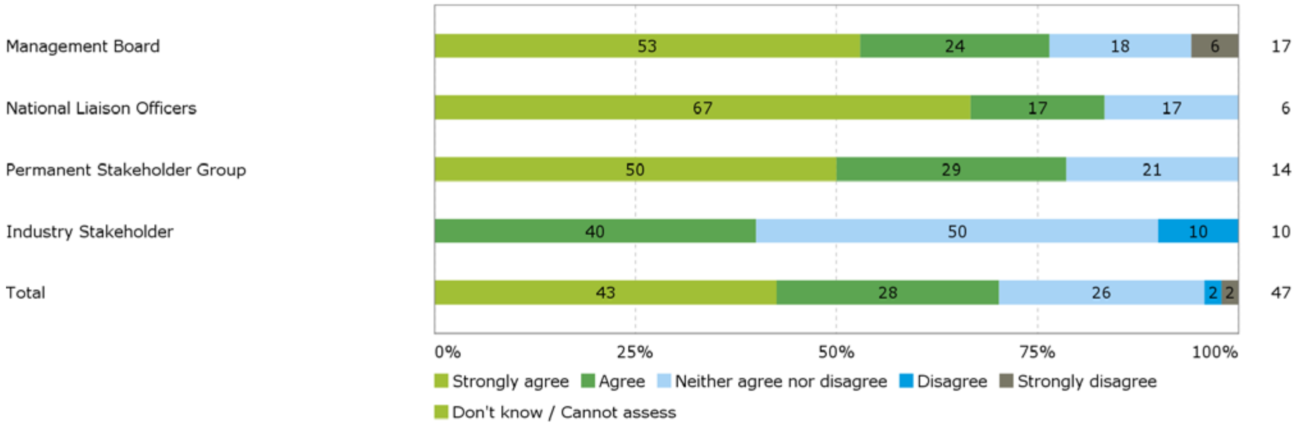
4.2 ENISA effectively supports the sharing of information, ideas and common areas of interest among stakeholders



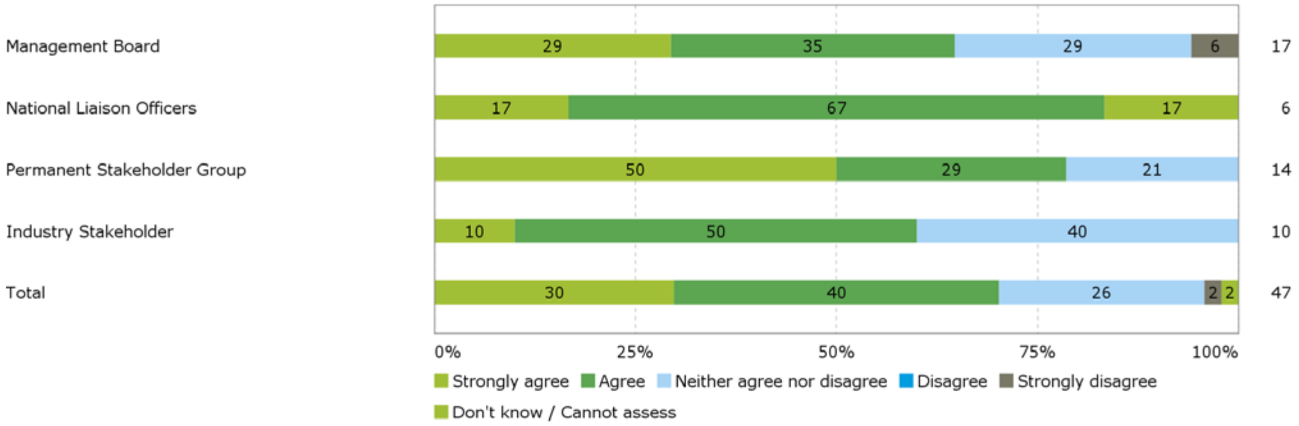
4.3 ENISA's support to cooperation between stakeholders complements other public interventions



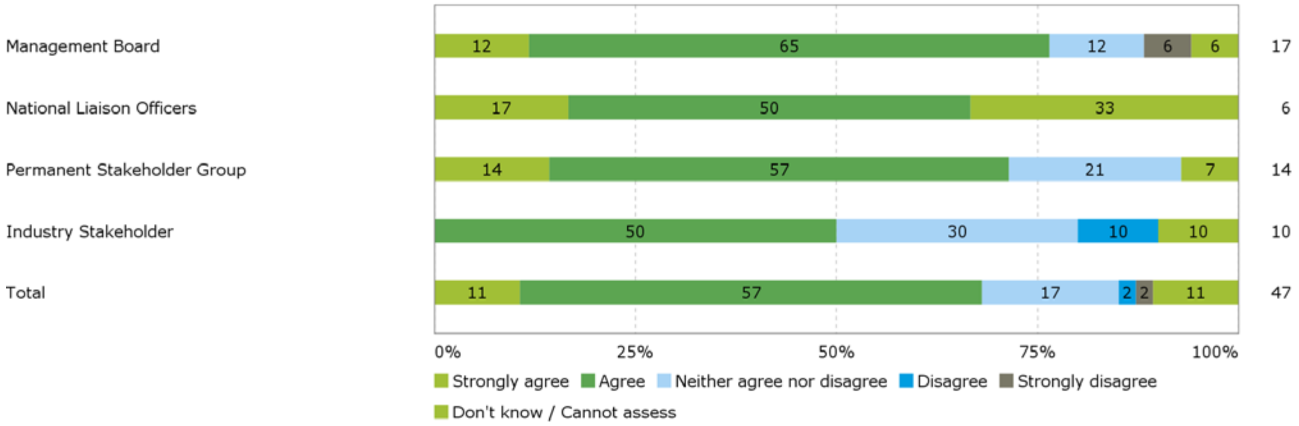
4.4 ENISA effectively shares lessons learned from cyber exercises with other communities and sectors



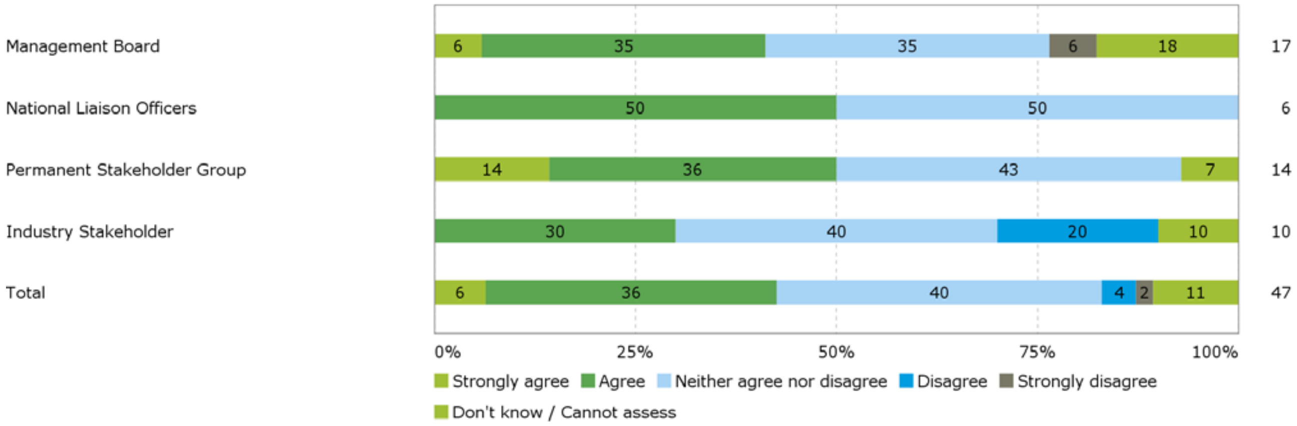
4.5 ENISA’s support has contributed to enhanced cooperation in operational communities



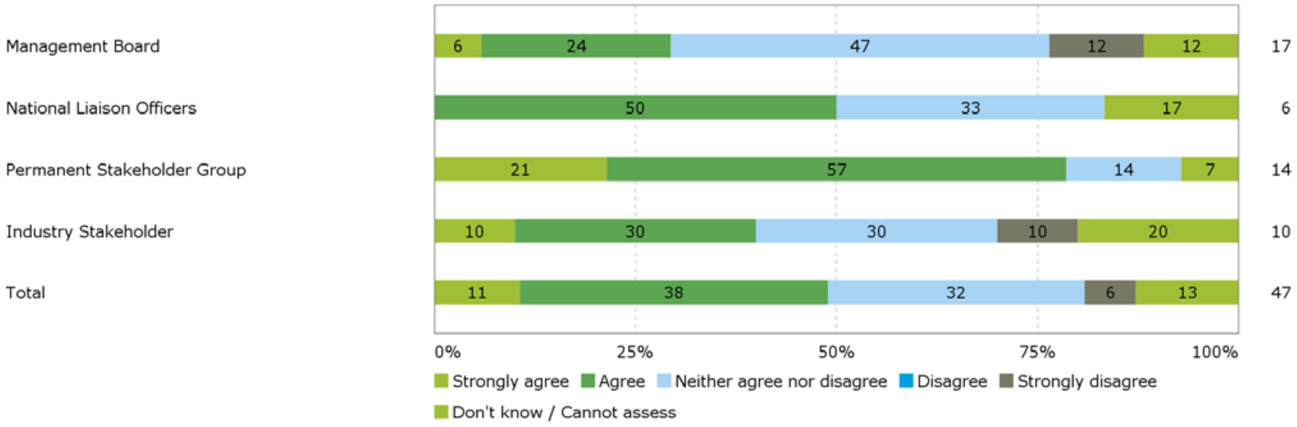
4.6 ENISA’s support has improved services, workflow and communication among stakeholders to respond to crises



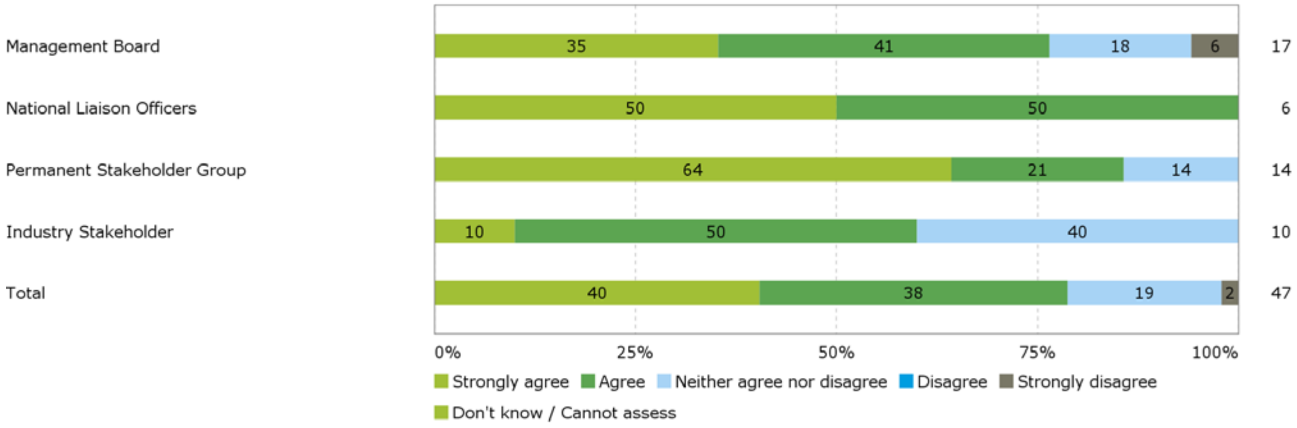
4.7 Technical capacity has increased among involved stakeholders



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



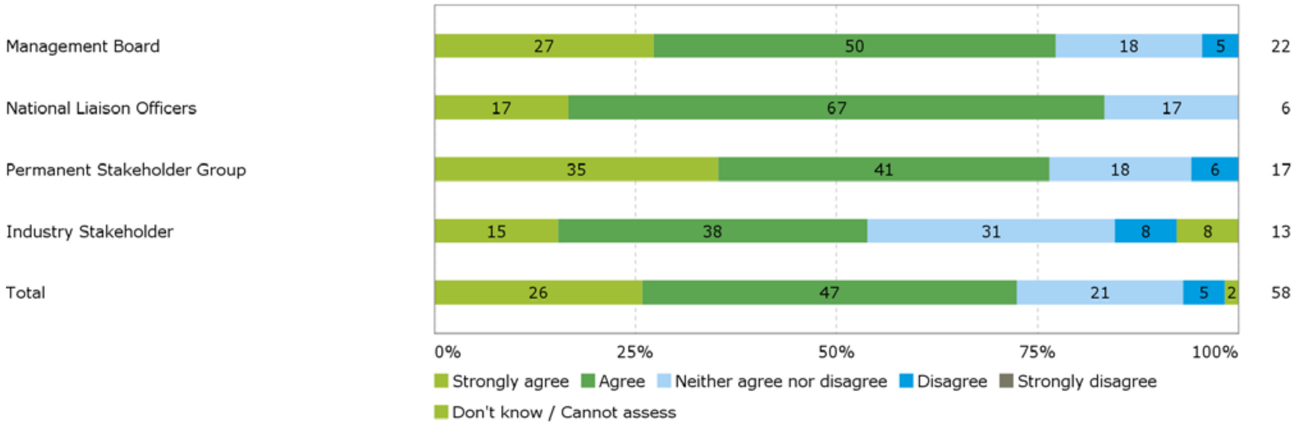
4.10 Please provide additional comments as relevant:

Management Board / National Liaison Officers	Permanent Stakeholder Group / Industry stakeholders
• More resources needed and more attention by MS at a senior level	• ENISA's relationship with senior decision makers in the Member States needs to be developed. • ENISA should have better instruments to help industry to come together to share experiences, best practices, projects... to build up a strong and resilient ICT sector in EU • ENISA achieved excellence in creating a community of practice that links various stakeholders; its contribution here is invaluable.

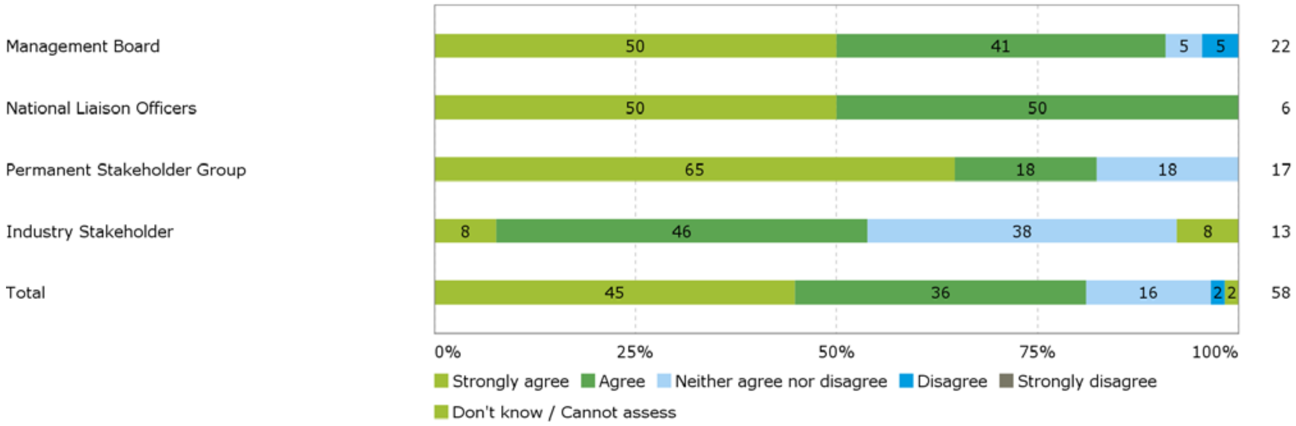
5. IMPACT OF ENISA'S SUPPORT

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

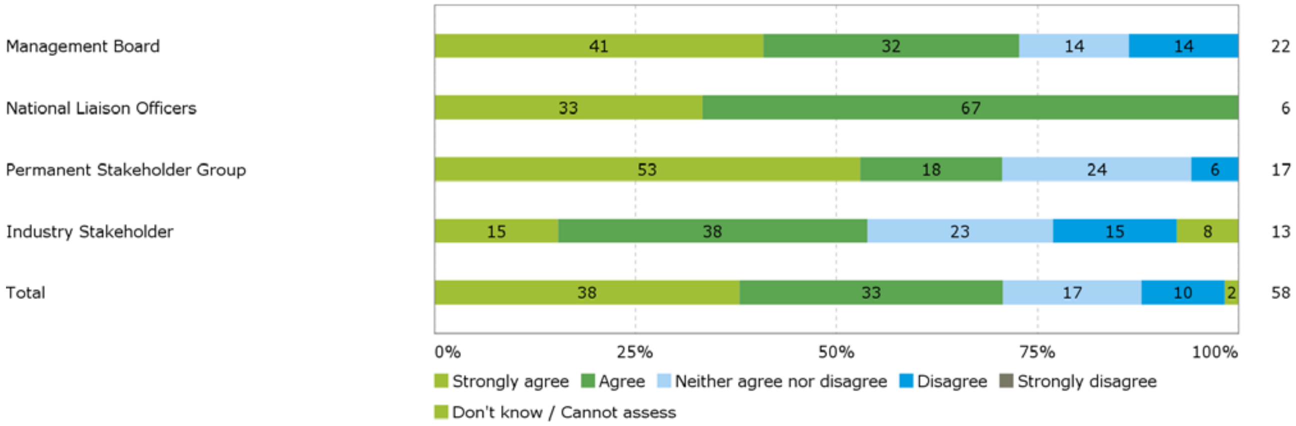
5.1 ENISA clearly contributes to ensuring a high level of NIS within the EU



5.2 ENISA clearly contributes to raising awareness on 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:

Management Board / National Liaison Officers	Permanent Stakeholder Group / Industry stakeholders
-	• ENISA's facilitation role restricts its ability to meet ambitious objectives. • ENISA does not have enough funding to achieve EU society in general to build up a culture of NIS or raising awareness. • This is very important. I think it's too little. Just having a cyber-security month is not sufficient

1. DO YOU HAVE ANY PARTICULAR SUGGESTIONS AS TO HOW ENISA COULD IMPROVE IN THE FUTURE?

Management Board / National Liaison Officers	Permanent Stakeholder Group / Industry stakeholders
• Create a new work program from the scratch, adapted to 2015 and not dragging initiatives from 2014 • resources are too limited; thus ENISA should concentrate on quality not quantity • A better integration and coordination of all it-security relevant instruments and activities with ENISA as the primary knowledge base would be very helpful. • ENISA could do more work on security of cryptographic algorithms	• A more hands on approach with Member States with a view to developing capabilities and practices is desired. This would involve a more operational role coupled with a more interventionist approach involving mentoring, assessment and auditing of capabilities subject to political constraints and rights of individual Member States. • Cyber Threat Intelligence Risk Management methodologies, to address the various operational risks • Being involved with EU industry and build up together better resilient capabilities • The EU community must extend and strength the capacities and skills of ENISA to play really a central role in the field of NIS to coordinate the management of cyber security activities in Europe and set up an effective risk management. • Regarding awareness raising among the general public, it would be best to have ENISA-promoted information campaigns in mass media (main TV channels in each Member State, main newspapers, radio stations). There is a similar campaign in Korea by the Korean Information Security Agency that is well targeted at the citizen. Regarding ENISA services for companies, this should focus on reaching out to SMEs. Large companies have the capacity (resources and knowledge) to manage their own IT security, while SMEs do not. • Increase its visibility inside and outside the EU organisations. • In my humble opinion it's recommendable increase the technical skills of ENISA • I think ENISA both have good and relevant resources, services and reports/standards/. But too few stakeholders are aware of ENISA and their resources etc. Maybe have closer collaboration/cooperation/communication with key stakeholders in member states. Arranging annual conference including training (whole/half-day before or after conference) on info sec and ENISA products/services, Meet the experts, etc. • Upgrade to the resources needed. ENISA is still one of the smallest EU agencies, even though its mandate is so important. • Further closer links , cooperation and dialogue with genuine EU cyber security companies • I would suggest greater reliance on existing stakeholders and additional liaisons with key organizations to ensure

	broader dissemination of ENISA's excellent work. Also, while ENISA's focus on EU issues is necessary, greater participation in global issues will be helpful in favourably positioning EU in a variety of fields, from technology expertise and business development to policy.

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

Table 5 Evaluation matrix

Evaluation Question	Indicators	Judgement criteria	Data sources	Score board 2014
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	N/A
To what extent is ENISA's organisation conducive to support 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 (staff and management)	🟨
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	Interviews (staff and management)	🟨
Impact				
To what extent do ENISA's core operational activities contribute to	A high level of NIS within the EU is ensured	At least 70% of evaluation/survey respondents are of the opinion that	Yearly stakeholder surveys	🟩

Evaluation Question	Indicators	Judgement criteria	Data sources	Score board 2014
achieving more long term objectives (impact)?		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	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	N/A
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 (staff and management)	🟨
Coordination and coherence				
To what extent does ENISA coordinate activities with relevant bodies, offices and agencies in the field of Information and Communications Technologies (ICT)?	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	🟩
To what extent does ENISA's activities	View of other public stakeholders on	At least 70% of evaluation/survey	Yearly stakeholder surveys	🟩

Evaluation Question	Indicators	Judgement criteria	Data sources	Score board 2014
contradict or complement those of other public interventions?	ENISA's complementarity with other public interventions Any adverse effects from ENISA's work	respondents are of the opinion that ENISA complements other public interventions No adverse effects identified	Interviews with stakeholders	🟩

Table 6 Work stream 1 Support to EU Policy Building

ENISA's objectives outcome and results level	Indicator	Score board 2014[30]	Target	Data sources
Deliverables 2014 Work stream 1 Support to EU Policy Building				
WPK 1.1-D1 Annual EU Cyber Security Threats and Landscapes	Resources used for research and publication (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK1.1-D2 Identification of trends, security challenges, associated risks and required countermeasures	Resources used for research and publication (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK 1.2-D6 Algorithms and parameters for secure services	Resources used for research and publication (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK 1.3-D1 Inventory of standardisation activities in NIS and privacy	Resources used for research and publication (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
Outcome indicators				
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.	🟩	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 were relevant	Yearly stakeholder surveys Interviews
	MS' views on the degree to which ENISA's deliverables complement those of other public interventions	🟩	At least 70% of evaluation/survey respondents are of the opinion that the deliverables complement those of other public interventions	Yearly stakeholder surveys Interviews

[30] ≥70%:green, 51 – 69%:yellow, ≤50%

ENISA's objectives outcome and results level	Indicator	Score board 2014[30]	Target	Data sources
		🟩	Staff/stakeholders interviewed are of the opinion deliverables complement those of other public interventions and provide examples to support this	
Input for new policy initiatives is provided	Policy makers views on the usefulness of the input from ENISA to develop new policies	🟩	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
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	🟩	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
Stakeholders are informed of new standardisation, innovation and research activities	Policy makers and public or private sector organisations views on the information provided by ENISA on standardisation, innovation and research	🟨	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
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	🟨	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
	Achievement of relevant KIIs	🟩	Targets achieved	Annual report 2014
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	🟥	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	Yearly stakeholder surveys Interviews

ENISA's objectives outcome and results level	Indicator	Score board 2014[30]	Target	Data sources
		🟥	contributes to the objective	
Standards for NIS and Privacy are set	Stakeholders views on ENISA's outputs contribution to setting standards for NIS and privacy	🟨	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

Table 7 Work stream 2 Capacity building

ENISA's objectives at outcome and result levels	Indicator	Score board 2014	Target	Data sources
Deliverables 2014 Work stream 2 Capacity Building				
WPK2.1-D2 White Paper – How to Evaluate National Cyber Security Strategy	Resources used for research/trainings and publication (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK2.1-D5 New set of CERT exercise material with at least five new scenarios from the four areas of the "baseline capabilities"	Resources used for research/trainings and publication (staff or cost) Satisfaction of participants		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014 ENISA evaluation form
WPK 2.1-D6 Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work	Resources used for research/trainings and publication (staff or cost) Satisfaction of participants		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014 ENISA evaluation form
WPK 2.2-D2 White Paper on the Certification of Smart Grids	Resources used for research/trainings and publication (staff or cost) Satisfaction of participants		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014 ENISA evaluation form
WPK 2.2-D5 Minimum Security Measures for Cloud Computing	Resources used for research/trainings and publication (staff or cost) Satisfaction of participants		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014 ENISA evaluation form
WPK 2.2-D7 Guidelines for the identification critical services, assets and links in electronic communication networks	Resources used for research/trainings and publication (staff or cost) Satisfaction of participants		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014 ENISA evaluation form
WPK2.2-D8 Guidelines for secure inter-banking communications and transactions	Resources used for research/trainings and publication (staff or cost) Satisfaction of participants		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014 ENISA evaluation form
Outcome indicators				
Good practices regarding cybersecurity are disseminated among public and private organisations	Public and private stakeholders agree that good practices have been disseminated by ENISA	🟩	At least 70% of evaluation/survey respondents are of the opinion good practices have been disseminated Staff/stakeholders interviewed are of	Yearly stakeholder surveys Interviews

		🟩	the opinion that good practices are disseminated	
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	🟩	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
The state of preparedness of the private sector community is improved	Private and public stakeholders’ views on the preparedness of the private sector thanks to ENISA’s support	🟨	At least 70% of evaluation/survey respondents are of the opinion that preparedness has been improved thanks to ENISA’s support Staff/stakeholders interviewed are of the opinion that the private sector’s preparedness is improved	Yearly stakeholder surveys Interviews
	Stakeholders’ views on the degree to which ENISA’s outputs complement those of other public interventions	🟩	At least 70% of evaluation/survey respondents are of the opinion that the outputs complement those of other public interventions Staff/stakeholders are of the opinion that outputs complement those of other public interventions and provide examples to support this	Yearly stakeholder surveys Interviews
Result indicators				
Public and private stakeholders are prepared to coordinate and cooperate with each other during a cyber crisis	Stakeholders’ views on the degree to which they are prepared to coordinate and cooperate during a cyber-crisis	🟩	At least 70% of evaluation/survey respondents are of the opinion that they are prepared Staff/stakeholders interviewed are of the opinion that preparedness is good	Yearly stakeholder surveys Interviews
	Achievement of relevant KIIs	🟩	Targets achieved	Annual report 2014
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	🟩	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
	Achievement of relevant KIIs	🟩	Targets achieved	Annual report 2014

Cyber security challenges are addressed	Stakeholders' views on the degree to which cyber security challenges are adequately addressed	🟥	At least 70% of evaluation/survey respondents are of the opinion that cyber security challenges are adequately addressed Staff/stakeholders interviewed are of the opinion that cyber security challenges are adequately addressed	Yearly stakeholder surveys Interviews
	Achievement of relevant KIIs	🟩	Targets achieved	Annual report 2014

Table 8 Work stream 3 Support Cooperation

ENISA's objectives at outcome and result levels	Indicator	Score board 2014	Target	Data sources
Deliverables 2014 Work stream 3 Support Cooperation				
WPK3.1-D1 Cyber Europe 2014: Exercises Plan and Exercise	Resources used (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK3.1-D2 Report on Cyber Crisis Cooperation and Exercise Activities and Findings	Resources used (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK3.2-D1 Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents	Resources used (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK 3.3-D2 Good governance guide and/or training and exercise material for the exchange and processing of actionable information CERTs	Resources used (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
WPK3.3-D3 Draft report "Stocktaking on channels and formats for exchange of operational information"	Resources used (staff or cost)		N/A – tracking/comparison against year 1.	Financial data from ENISA Annual report 2014
Outcome indicators				
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	🟩	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

ENISA’s objectives at outcome and result levels	Indicator	Score board 2014	Target	Data sources
		🟩	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	🟩	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
Lessons learnt from exercises are shared with other communities and sectors	Stakeholders agree that lessons learned from exercises are shared with other communities and sectors	🟩	At least 70% of evaluation/survey respondents are of the opinion that lessons learned from exercises are shared with other communities and sectors Staff/stakeholders interviewed are of the opinion that lessons learned from exercises are shared with other communities and sectors	Yearly stakeholder surveys Interviews
The implementation of Art. 13a and Art.4 as well as synergies between the two are supported	KIIS on the support of Art 13.a and Art. 4.	🟩	KIIs achieved	Annual report
Cooperation between operational communities is enhanced	Stakeholders views on enhanced cooperation in operational communities	🟩	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
New potential target groups for ENISA deliverables are identified	New target groups are continuously identified and included in dissemination activities	🟩	Staff/stakeholders interviewed are of the opinion that new target groups are continuously identified and included in dissemination activities	Interviews
Result indicators				
Member States, EU institutions and other players improve services, workflows and communication to respond to	Stakeholders’ views on the degree to which services, workflow and communication to respond to crisis has been improved	🟨	At least 70% of evaluation/survey respondents are of the opinion that services, workflow and communication to respond to crisis has been improved	Yearly stakeholder surveys Interviews

ENISA's objectives at outcome and result levels	Indicator	Score board 2014	Target	Data sources
emergency cases		🟨	Staff/stakeholders interviewed are of the opinion that services, workflow and communication to respond to crisis has been improved	
	Technical capacity has increased among involved stakeholders	🟥	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 2014
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	🟥	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 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	Yearly stakeholder surveys Interviews Incident reports
Community building in Europe and beyond is enhanced	Stakeholders' views on the degree to which community building in Europe and beyond is enhanced	🟩	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

Work stream 1: Support EU policy building

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
WPK 1.1 Identifying evolving threats, risks and challenges	D1	Annual EU Cyber Security Threats Landscapes	The ENISA Threat Landscape is referenced in at least 10 security related information sources worldwide. It is referenced by 5 stakeholders form the 2 sectors covered. At least 5 R&D projects in the EU take identified emerging threats and trends into consideration.	Achieved: More than 20 different organisations are using the conclusions of ENISA's Threat Landscape report 2014. Several hundred references to ENISA Threat Landscape 2013 have been made via the main cyber security web pages and blogs. Both ENISA thematic threat landscapes have been referenced by couple of tens of stakeholders from Internet infrastructure, smart home and converged media sectors. Most of the threats identified in ENISA thematic landscapes have been addressed in various H2020 projects.	ENISA Threat Landscape 2014	13,002
	D2	Identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/ sectors)			Threat Landscape and good practice guide for smart home and converged media; Threat Landscape and good practice guide for Internet infrastructures	3,705 4,308
WPK1.2 Contributing to EU policy initiatives	D3	Algorithms and parameters for secure services (study)	ENISA recommendations on algorithms and parameters for secure services for the protection of personal data in the context eGov services are supported by competent authorities in at least 5 MS.	Achieved: The reports providing guidelines for securing personal data (cryptographic measures, privacy technologies) were produced in collaboration with well–known experts from different States and competent authorities. Feedback was provided by competent authorities. The reports are supported by competent authorities from more than five different Member States and standardisation bodies.	Algorithms, key size and parameters report 2014; Study on cryptographic protocols	10,046 6,660

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
WPK1.3 Supporting the EU in education, research and standardisation	D1	Inventory of standardisation activities in NIS and Privacy (workshop, report)	At least 5 members of the R&D community integrate NIS components in their activities and projects	Achieved: Representatives from 11 countries participated in the work undertaken by ENISA — workshops and reports. In 2014 various scenarios were developed, which will be further implemented during 2015.	Standardisation in the field of Electronic Identities and Trust Service Providers	1,695

Work stream 2: Support capacity building

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
WPK 2.1 Support Member States' capacity building	D2	White Paper - How to Evaluate National Cyber Security Strategy (report)	10 MS and 5 private companies support ENISA's conclusions on national cyber security strategies.	Achieved: The ENISA NCSS working group is comprised of 14 MS and 1 EU country and is actively contributing to the ENISA NCSS studies. More than 15 private companies (mostly from energy sector) support ENISA recommendations.	An evaluation framework for Cyber Security Strategies	12,747
	D5	New set of CERT exercise material with at least five new scenarios from the four areas of the "baseline capabilities", including the topic of processing of actionable operational information	Improved operational practices of CERTs training provided to a minimum of 20 participants of different organisations.	Achieved: In total more than 135 people were trained in the year 2014 (675% achievement); and the new CERT training material achieved around 20 000 unique page views (published Q4/2014), while for the existing material succeeded in attracting over 134,000 unique page views in 2014.	CERT exercise material: 1) Developing countermeasures; 2) Common framework for artefact analyses activities; 3) Advanced artefact handling; 4) Processing and storing artefacts; 5) Building an artefact handling and analyses environment	N/A

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
	D6	Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work in this area			Impact assessment and roadmap	1,357
WPK 2.2 Support Private Sector Capacity Building	D2	White Paper on the Certification of Smart Grids			Smart grid security certification in Europe; Validation workshop for 'Smart Grid Components Certification' reports organised on 30.09.2014	2,641
	D3	White Paper on the Certification of Cyber Security Skills of ICS SCADA experts	10 ICS-SCADA providers/manufacturers support ENISA's conclusions on the Certification of Cyber Security Skills of ICS-SCADA experts	Achieved: ENISA ran a working group with 15 experts from utilities manufactures vendors and public authorities. In addition ENISA supported and contributed to the EURO SCSIE group, a highly recognised WG on ICS SCADA security.	Recommendations for developing harmonised certification schemes at European level for Cyber Security Skills of ICS SCADA experts; Validation workshop for the 'Certification of cyber security skills of ICS SCADA experts' report organised on 30.09.2014	3,799
	D5	Minimum Security Measures for Cloud Computing	15 Cloud Computing Providers and 5 MS competent authorities contribute to ENISA's study on minimum security measures for cloud computing	Achieved: 20 Cloud providers and 12 Member States participated in the study for 'Cloud certification meta framework'.	Cloud Certification Schemes Meta Framework Cloud security guide for SMEs Security framework for governmental clouds	N/A 8,638 7,028
	D7	Guidelines for the identification of critical services, assets and links in electronic communication networks			Methodologies for the identification of critical information infrastructure assets	2,447

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
					and services	
	D8	Guidelines for secure inter-banking communications and transactions	10 Finance Sector IT Security/IT Auditors agree on ENISA's recommendations on secure interbanking communications and transactions	Achieved: 25 experts participated in EG FI which supported the ENISA study on 'Network and Information Security in the Finance Sector'. Eight MS are represented in this EG.	Network and Information Security in the Finance Sector — Regulatory landscape and Industry priorities	4,286
WPK2.3 Raising the level of preparedness of EU citizens		no deliverables above 30,000 EUR				

Work stream 3: Support co-operation

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
WPK 3.1 Crisis cooperation - exercises	D1	Cyber Europe 2014: Exercise Plan and Exercise	At least 24 EU MS and EFT countries confirm their support for Cyber Europe 2012. At least 80% of MS that are in the process of establishing National Contingency Plans by 2016 are supported by ENISA. At least 24 MS are familiar with the operational procedures during cyber crisis by 2016.	CE 2014 involved 1,400 experts and over 450 teams, with an equal representation of public and private sector teams. In the different phases of Cyber Europe 2014 there were 29 different participating countries (26 MS, 3 EFTA) and the EU Institutions. In the first phase of CE2014 (TLEx) over 600 experts were involved, coming from 214 teams representing both private and public sector institutions. In the second phase of CE2014 (OLEx) there were over 800 experts. Over 1,400 experts were involved in	Exercise organised on 30.10.2014	
	D2	Report on Cyber Crisis Cooperation and Exercise Activities and Findings			Report on Cyber Crisis Cooperation and Management	2,269

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
				the exercises in some way during CE2014. MS have declared their satisfaction with the exercise through evaluation surveys and through communications via the ENISA Management Board members and NLOs. One of the objectives of CE2014 was to give the opportunity to MS to test their national capabilities and procedures. Out of the 29 countries (EU and EFTA) that collectively participated in the first two phases of CE2014, all have confirmed that they have tested their national contingency plans and capabilities. The second phase of CE2014 mainly focused on testing the operational procedures for cyber security cooperation in Europe. All of the 26 countries that participated in this phase were trained to use these procedures. In addition, the countries that did not play in this phase had access to and received the updated version of the SOPs within the pilot SOP portal within the Cyber Exercise Platform.		

WPK 3.2 Implementation of EU legislation	D1	Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents	23 MS contribute to ENISA's work on the implementation of Article 13a and 12 MS directly use outcomes of this work by explicit references or by adopting the same approach nationally.	Achieved: All 28 Member States plus two EFTA Countries sent to ENISA and the Commission annual summary reports about incidents that occurred in 2013. All Member States use the ENISA Technical Guideline on Article 13a Incident Reporting in their annual reporting. More	Annual Incidents report 2013;
					Technical Guideline on Incident Reporting V2.1;
					Technical
						5,640
						3,343
						4,533
						1,110

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015

				than 12 MS and some of the larger European Electronic Communications Providers use directly or refer to the ENISA Technical Guideline on Security Measures. During 2014 ENISA has performed three workshops with the Article 13a Expert Group attended by NRAs from around 20 Member States.
				The participants in the ENISA Electronic Communications Reference Group consisting of 23 Providers support ENISAs work on a joint technical guidelines on Article 13a (Telecom Framework Directive) security measures and Article 4 (ePrivacy Directive) security measures.
					Guideline on Security Measures V2.0;
					Secure ICT Procurement in Electronic Communications;
					Security Guide for ICT Procurement;
					Protection of underground electronic communications infrastructure
						1,333
						1,239

WPK 3.3 Regular cooperation among NIS communities	D2	Good governance guide and/or (where applicable) training and exercise material for the exchange and processing of actionable information CERTs	At least 10 MS support the Good Practice Guide and/or training and exercise material for the exchange and processing of actionable information by CERTs	Achieved. The expert group included reviewers, commenters ENISA hosted teams from Siemens (Germany), SWITCH (Switzerland), Portugal (CERT.PT), Poland (CERT.PL), Austria (CERT.AT) Czech Republic (CESNET), from the US (CERT.CC and US‑CERT) international organisations like FIRST, NEC, NATO, NAIST, Invincea and the CSIRT Gadgets Foundation (13 teams altogether). In the BoF session at the FIRST conference 2014 many more teams provided input to the study.	Best practice guide on exchange processing of actionable information — exercise material	4,016
	D3	Draft report "Stocktaking on channels and formats for exchange of operational information"	10 operational CERTs agree to adopt the recommendations of stocktaking on	Achieved. Most of the EU teams use the same or similar concepts and models like the study laid out. Several	Stocktaking of standards formats used in exchange	

Work packages	No of deliverable	Title of deliverable	Impact indicator (according to Work Programme 2014)	Achieved results (according to Annual Activity Report 2014)	Publications and activities	Downloads up to June 2015
			channels and formats for exchange of operational information	discussions throughout the year addressing the CERT communities resulted in positive feedback from a minimum of 13 Member States (from several teams, among them from Portugal, Poland, Austria, Switzerland, Luxembourg, Romania, Denmark, Norway, Czech Republic, Germany, Latvia, Belgium, CERT–EU, etc.)	of processing actionable information	