EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 502 final

COMMISSION STAFF WORKING DOCUMENT

on the evaluation of the European Union Agency for Network and Information Security (ENISA)

Accompanying the document

Proposal for a regulation

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

{COM(2017) 477 final}
{SWD(2017) 500 final}
{SWD(2017) 501 final}

Table of Contents

1. INTRODUCTION

The European Agency for Network and Information Security (ENISA) was originally established in 2004 and had its mandate renewed periodically. The current ENISA mandate is set out in Regulation EU No. 526/2013[1] (the 'ENISA Regulation') and is due to expire in June 2020.

Article 32 of the ENISA Regulation requires the Commission to conduct an evaluation to assess in particular the impact, efficiency and effectiveness of the Agency and its working practices by 20th June 2018. Furthermore the evaluation results are to inform the Commission as to whether it is to propose that the duration of the current mandate be extended.

In its 2016 Communication "Strengthening Europe's cyber resilience system and Fostering a Competitive and Innovative Cybersecurity industry"[2], the Commission announced that, taking also into account the reinforced role that the NIS Directive attributes to the Agency, it will advance its evaluation and, subject to the results of such evaluation, it would present a proposal for a possible new mandate as soon as possible. In its Communication on the DSM Strategy Mid-term Review of May 2017[3], the Commission has further specified that, it would review the mandate of ENISA, included in its Work Programme, by September 2017 in order to define its role in the changed cybersecurity ecosystem.

The evaluation falls under the Commission's Regulatory Fitness and Performance Programme (REFIT). It has been conducted according to an evaluation roadmap[4] that was made public in July 2016.

The Commission concluded a tender with a consortium led by CARSA5, to provide an independent evaluation of ENISA in autumn 2016 (Annex 4). The present Staff Working Document is largely based on the results and conclusions of that evaluation study.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1495472820549&uri=CELEX:32013R0526
[2] COMM (2016)410 final.
[3] Commission Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy - COM(2017) 228.
[4] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf
[5] Consortium includes CARSA (Consultores de Automatización y Robótica S.A. - lead partner), Logotech (partner), Ramboll Management Consulting S/A (partner), AIT Austrian Institute of Technology GmbH (partner), ZSI – Zentrum für Soziale Innovation (partner) and Agilis S.A. (partner).

1.1. Purpose of the Evaluation

The purpose of the evaluation of ENISA was to assess the performance of the Agency in achieving its objectives, mandate and tasks, as laid down in the Regulation No 526/2013 and to provide the basis for a possible revision of the current mandate. Its results fed the impact assessment regarding the future of ENISA.

In compliance with the Better Regulation Guidelines, the evaluation has assessed the effectiveness, efficiency, coherence, relevance and EU added value of the Agency, having regard to its performance, governance, internal organisational structure and working practices.

The analysis also took account of the evolved context where the Agency now operates, with regard in particular to: the new EU regulatory and policy framework (e.g. the NIS Directive, the Review of the EU Cybersecurity Strategy); the evolving needs of the Agency's stakeholders' community; and the complementarity and possible synergies with the work conducted by other EU and national institutions, agencies and bodies, such as CERT-EU and the European Cybercrime Centre (EC3) at Europol.

The present Staff Working Document will accompany the Commission Report to the European Parliament and the Council to allow for a decision how to pursue the recommendations made.

1.2. Scope of the Evaluation

The legal basis for this evaluation is set out in article 32 of ENISA's Regulation.

In particular, the main objectives of the evaluation have been:

1. to assess the effectiveness, efficiency, relevance, coherence and EU value added of the work undertaken by the Agency and its working practices. The assessment has sought to evaluate, but not be limited to, the implementation of the work programme as well as how the whole set of activities run by ENISA (including opinions, guidelines, trainings, recommendations or reports) have contributed to fulfil its role, objectives, mandate and tasks.
2. to assess how effectively the current governance as well as the internal organisational structure of ENISA (Management Board-MB, Executive Board, Executive Director and staff and Permanent Stakeholders Group -PSG) have contributed to efficiency and effectiveness in the work of ENISA. The assessment of the organisational structure has also included an evaluation of the efficiency and effectiveness of the current arrangements related to the location of ENISA's offices.
3. to assess how successfully ENISA, within its mandate, has met the needs of its constituency in comparison to other EU and national bodies working on cybersecurity.
4. to assess the possible need for a revision or extension of the mandate entrusted to ENISA, also taking into account the evolution of the cybersecurity and digital privacy landscape, including the regulatory and policy framework (in particular the adoption of the NIS Directive and the current review of the Cybersecurity Strategy).

The time period covered by the evaluation is 2013 – 2016 but data and information were collected and analysed also in 2017. The analysis in fact starts with the entry into force of the Regulation No 526/2013, which set the new mandate for ENISA and concludes with issuing of the DSM Strategy Mid-term Review of May 2017, where the Commission has further specified that it would review the mandate of ENISA by September 2017 in order to define its role in the changed cybersecurity ecosystem. In terms of geographical scope, the evaluation assessed the impact of ENISA on all 28 Member States.

2. BACKGROUND TO ENISA

2.1. Description of the ENISA Mandate

ENISA was established in 2004 (Regulation (EC) No 460/2004) as the European Union Agency for Network and Information Security with the objective of facilitating a high level of network and information security within the EU. The Agency was established in the context of the new emerging digital economy and the need to safeguard its development. The initial foreseen duration for the Agency's mandate was 5 years but it was extended twice (in 2009 and 2011).

The current mandate of the Agency is set out in Article 1 of Regulation EU n. 526/ 2013 (which repealed the 2004 Regulation and represents the new basic Act for ENISA): *"to undertake the tasks assigned to it for the purpose of contributing to a high level of network and information security within the Union and in order to raise awareness of network and information security and to develop and promote a culture of network and information security in society for the benefit of citizens, consumers, enterprises and public sector organisations in the Union, thus contributing to the establishment and proper functioning of the internal market".* ENISA can only intervene where it does not impact on the national competence of Member States in regard to network and information security matters such as national security, defence, public security and criminal law matters.

ENISA's objectives are defined by article 2 of its Regulation, namely:

1. The Agency shall develop and maintain a high level of **expertise**.

2. The Agency shall assist the Union institutions, bodies, offices and agencies in **developing policies** in network and information security.

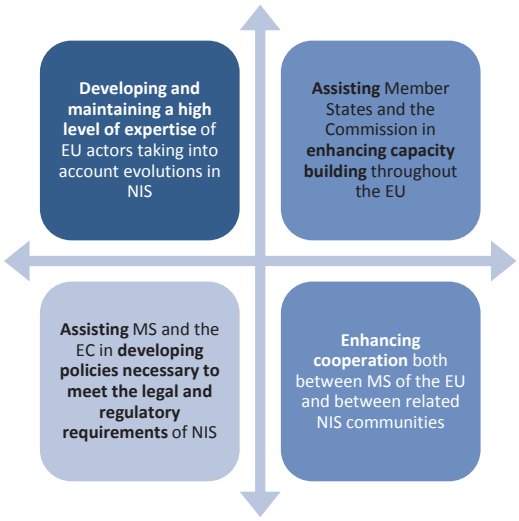
3. The Agency shall assist the Union institutions, bodies, offices and agencies and the Member States in **implementing the policies** necessary to meet the legal and regulatory requirements of network and information security under existing and future legal acts of the Union, thus contributing to the proper functioning of the internal market.

4. The Agency shall assist the Union and the Member States in enhancing and **strengthening their capability** and preparedness to prevent, detect and respond to network and information security problems and incidents.

5. The Agency shall use its expertise to **stimulate broad cooperation** between actors from the public and private sectors.

ENISA's understanding of these objectives is set out in the diagram overleaf.

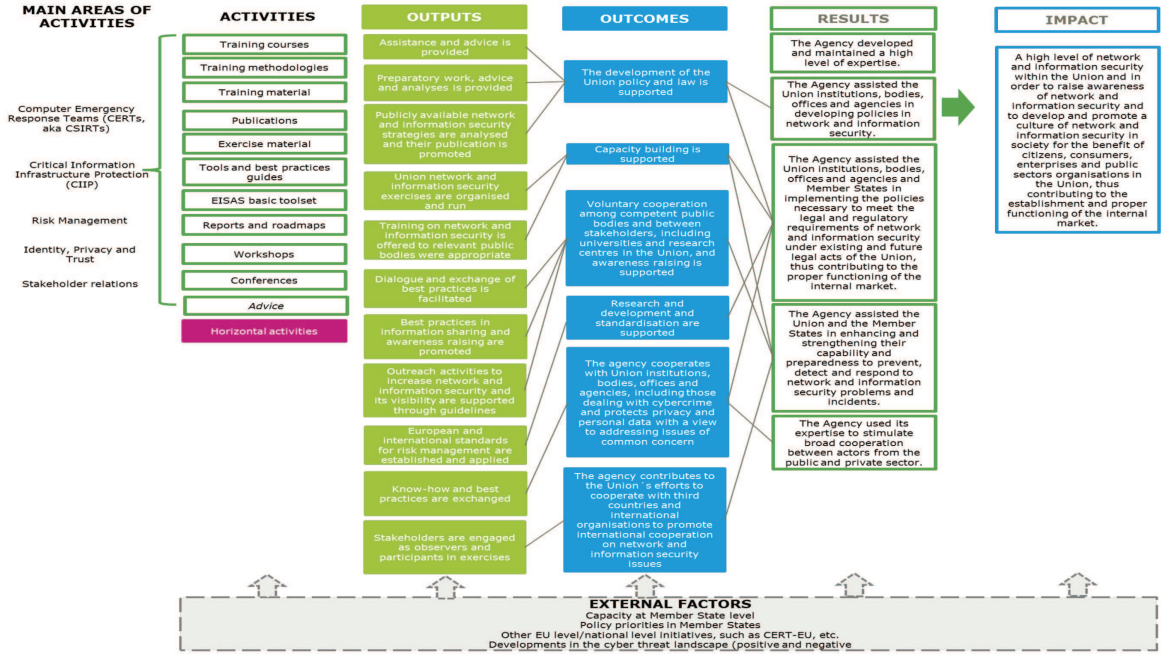
Figure 1 ENISA's activities based on its objectives



Source: Ramboll Management Consulting based on ENISA Website

For ENISA to achieve its objectives, the Regulation identified a list of tasks, as well as operational, governance, organisational and financial provisions. The problems ENISA is intended to address are set out in detail in the baseline section. The diagram below (figure 2) summaries how ENISA as an Agency is intended to address the core issues such as lack of knowledge, expertise, trust and the resulting limited co-operation.

Figure 2 ENISA's Intervention Logic Diagram



Source: Ramboll Management Consulting

ENISA is governed by a Management Board (MB) consisting of representatives from each of the 28 Member States and the Commission. A subgroup of the MB forms the Executive Board and it is tasked with routine decision making in the interests of administrative efficiency. An Executive Director appointed by the Management Board is responsible for managing the Agency. A Permanent Stakeholders Group (PSG) of

experts from industry, academia and consumer organisations advises the Agency in regard to the performance of its activities. The Agency also maintains an informal network of National Liaison Officers from the Member States to promote the Agency and facilitate outreach.

2.2. Baseline

The current ENISA Regulation has repealed the 2004 founding act of the Agency and the situation before its adoption is considered as baseline for the purpose of the evaluation.

Before 2004, prior to the existence of ENISA, there was no European focal point regarding network and information security. Furthermore, some Member States were not only devoting limited resources to network and information security capacity building, but were not sufficiently aware as to the importance of security and resilience of information communications technologies. There was no EU level advice or support mechanism to assist the Member States or the EU institutions, agencies and bodies become more aware of the critical issues related to secure and resilient digital infrastructure and services.

In the period 2004 – 2013, the EU had benefited from the establishment of an agency mandated to contribute to network and information security, helping Member States and the business community to prevent, to address and to respond to major network and information security risks. The mandate had not been substantially changed during this time frame but simply extended with regard to its duration.

However, the fast evolving nature of the cybersecurity domain, which was slowing becoming also a policy priority at EU and national level, made the previous mandate of ENISA outdated. In fact, by 2013, the centrality of the smartphone, the proliferation of mobile apps and the increasing reliance of public services (e.g. energy generation, transportation, etc.) on digital technologies required a renewed focus on network and information security. That year saw the publication of the first EU Cybersecurity Strategy[6], accompanied with a proposal for a Directive on Network and Information Security (the 'NIS Directive').

As reported in the impact assessment accompanying the 2013 legislative proposal, throughout the debate on the future NIS policy in Europe the Member States and various stakeholders repeatedly expressed the view that a modernised NIS agency was needed to best serve the goals of a renewed NIS strategy. In particular, the tasks defined by the previous ENISA Regulation were considered insufficient to provide the Agency with the necessary flexibility and adaptability to respond to the challenges of the continuously evolving NIS environment.

The renewal of the ENISA mandate in 2013 addressed also the internal governance and operations of the Agency (i.e. an Executive Board to aid decision making, a requirement for a branch office in Athens to increase operational efficiency). An effort was made to make the mandate flexible enough to respond to the evolving threat landscape but no substantive changes were made to the key objectives and the Agency was again entrusted with a fixed-term mandate (until 2020). This followed the rapid development of the

[6] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667 Cybersecurity Strategy for the European Union: An Open Safe and Secure Cyberspace JOIN 2013 (1) final 7 Feb. 2013

Agency from a start-up situation in 2004. By the end of 2012, ENISA had 58 staff members and an annual operating budget of approx. € 8.2 million[7].

3. IMPLEMENTATION STATE OF PLAY

Based on the mandate entrusted to it, ENISA supports the European Institutions, the Member States and the business community in **addressing, responding and especially preventing network and information security problems**. It does so through a series of activities across five areas identified in its strategy[8], adopted by the Management Board in 2016:

- expertise: provision of information and expertise on key network and information security issues.
- policy: support to policy making and implementation in the Union.
- capacity: support to capacity building across the Union (e.g. through trainings, recommendations, awareness raising).
- community: foster the network and information security community [e.g. support to the Computer Emergency Response Teams (CERTs), coordination of cyber exercises].
- enabling (e.g. engagement with the stakeholders and international relations).

ENISA carries out its activities according to an annual and multiannual work programme[9]. Every year, the Executive Director puts forward a proposal for the annual work programme, including a multiannual outlook on the strategic objectives and the resources. The resulting programming document is discussed by the Management Board and the Permanent Stakeholder Group provides an opinion to the Executive Director. The Commission also provides an official opinion based on the draft approved by the Management Board.

ENISA regularly executes its work programmes according to the planning. The latest Work Programme (WP 2016) has resulted in 64 deliverables executing in full the planning. The results of each work programme are presented by the Executive Director in annual activity reports, which in the period under consideration (2013-2016) have been adopted unanimously and on time by the Management Board.

The Executive Director also commissioned annual external evaluations[10] of the Agency, the conclusions of which fed follow-up action plans. The progress on the follow-up action plans has been reported annually to the Management Board and the Commission, indicating where no specific action had been taken due to management decision or lack of resources.

[7] ENISA General Report 2012, position on 31/12/2012
[8] https://www.enisa.europa.eu/publications/corporate/enisa-strategy
[9] https://www.enisa.europa.eu/publications/corporate/enisa-work-programmes-general-reports
[10] https://www.enisa.europa.eu/about-enisa/annual-ex-post-evaluation-of-enisa-activities

In recent years, ENISA has gained responsibilities involving the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), the Telecommunications Framework Directive and the ePrivacy Directive around security and reporting requirements.

Furthermore, under the Directive on Security of Network Information Systems (the 'NIS Directive', adopted in 2016), the Agency has gained significant new responsibilities involving assistance to Member States and its involvement in both the NIS Cooperation Group and as secretariat of the CSIRT Network, the two fora being responsible for EU cybersecurity cooperation at strategic and operational level respectively (articles 7, 9, 11, 12 and 19 of the NIS Directive).

ENISA has today 84 staff members, of which 48 Temporary Agents, 30 Contract Agents and 5 Seconded National Experts. Its offices are located in Greece, notably the administrative seat in Heraklion (Crete) and the core operations department in Athens. ENISA's annual budget increased by 16% over the period 2013 to 2016, amounting to 10.5m€ in 2016; in 2017 its budget was raised to 11.25 m€. The revenue of the Agency derives mostly from the EU budget, to which an annual contribution is added from the Greek authorities for the rental costs of its offices and a contribution from EFTA countries.

4. METHOD

The evaluation process was assisted by a **Steering Group** composed of the representatives of the European External Action Service and selected Commission Directorates General (DGs) including DG CNECT, DG HOME, DG JUST, DG JRC, DG DIGIT, DG HR, DG BUDG, together with the Secretariat-General and the Legal Service.

The Group steered and monitored the progress of the exercise, ensuring the necessary quality, impartiality and usefulness of the evaluation.

The evaluation was supported by an external comprehensive study. The contractors were given the task of collecting data and evidence in order to answer the evaluation questions set out in annex 3.

During the preparation phase of the study, familiarisation interviews took place with the Commission services[11] and CERT-EU at the commencement of the study. This was supplemented by preliminary desk research covering legal, policy and academic documents of relevance to the study.

Extensive desk research, as part of the data collection phase, on both primary and secondary sources was then conducted to capture the legal and regulatory landscape involving Commission Communications, Regulations and Directives, the work outputs of the Agency (i.e. workshop reports, conference publications, study findings) reports from the cyber security stakeholders (industry white papers, indices, public policy papers, expert groups etc) and websites, blogs and databases. The study then conducted in-depth interviews of up to 90 minutes each with 49 persons drawn from the cybersecurity stakeholders. This involved ENISA staff and management, Member State representatives (including some involved in the governance of ENISA), industry representatives, staff of

[11] DG-CNECT, DG-DIGIT

the Commission, other EU Agencies, Members of the European Parliament and CSIRTs. Industry, consumer representatives and civil society also participated. A stakeholder online survey was distributed to CSIRTs in all 28 Member States and CERT-EU to gather views and input on ENISA.

The study also carried out a benchmarking excercise of ENISA relative to other EU Agencies such as CEPOL, BEREC etc[12], a positioning exercise including some national cyber security agencies from large Member States[13] and an assessment of strengths, weaknesses, opportunities and threats (SWOT), validation of collected interview and survey data with secondary sources and a stakeholder workshop.

The study was supplemented by qualitative analysis carried out by the Commission through discussions and targeted consultations of key stakeholders. The Commission also carried out an open public consultation, in accordance with the requirements of the Better Regulation Guidelines.

The public consultation opened on 18th January and closed on 12th April 2017. 90 responses were received, from 19 Member States. A copy of the questionnaire used in the public consultation and a synopsis of the online public consultation is included in Annex 2.

The evaluation faced some **limitations** with regard to data collection, which were mitigated to the possible extent.

Among those limitations, the key impact indicators (KIIs) of the Agency set in the annual work programmes and reported upon in the annual activity reports change from one year to the next, limiting the possibility to implement a comparison of the Agency's outputs and results over the entire period of 2013-2016.

With a total of 90 responses, the results of the public consultation cannot be considered to be completely representative of all stakeholders concerned[14]. To overcome this weakness, further inputs from stakeholders were collected by the Commission. For example a roundtable organised by Commission Vice President Ansip in the context of the review of the cybersecurity strategy and discussion at the Council Horizontal Working Party on Cybersecurity were used to collect views from Member States.

Another limiting factor with the evaluation methodology was its reliance on stakeholder contribution. Some of them were part of ENISA's governance and organisation structures, that is to say staff, members of the Management Board, National Liaison Officers and Permanent Stakeholder Group representatives. The risk of possible bias was mitigated through triangulation of the data across different stakeholder groups and across the data collection tools. For example, the surveys and the interviews which primarily covered views from ENISA's staff, management and direct stakeholders were considered

[12] Full list includes Europol –European Cybercrime Centre (EC3),EU Agency for Fundamental Rights (FRA), Office of the Body of European Regulators for Electronic Communications (BEREC), European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), EU Agency for Law Enforcement Training (CEPOL) and European Fisheries Control Agency (EFCA).

[13] CERT-EU, Joint Research Centre of the EC (DG-JRC), Europol-EC3, Netherlands National Cyber Security Centre, Frency National Cybersecurity Agency (ANSSI) and Spanish National Institute for Cybersecurity (INCIBE).

[14] However, in the public consultation the views of national authorities of 15 Member States are represented. The private sector is represented by 27 respondents which include eight umbrella organisations, thus representing a significant number of European enterprises whose activities are linked with cybersecurity.

against the public consultation results and the workshop where a broader scope of stakeholders have been reached.

There was limited input from some cyber security stakeholders in industry and in public authorities who were not directly part of ENISA's outreach[15]. The study responded by undertaking in-depth interviews with 4 industry representatives, having 9 such interests attend the stakeholder workshop and taking account of the online public consultation (see above).

Based on the elements above, this evaluation has been carried out on the basis of the best available data.

5. RESPONSES TO THE EVALUATION QUESTIONS

The responses are grouped around the 5 key evaluation criteria as set out in the Better Regulation Evaluation Guidelines. A list of the individual evaluation questions is provided in Annex 3. The summary results are presented in table 1 below.

Table 1 Summary of results of the evaluation according to the criteria

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

Effectiveness

Summary: ENISA overall met its objectives and implemented its tasks. It made a contribution to increased NIS in Europe through its main activities (capacity building, provision of expertise, community building, support to policy). It showed potential for improvement in relation to each. However, ENISA faced difficulties to make a big impact in the vast field of NIS. This was also due to the fact it had fairly limited human and financial resources to meet a broad mandate.

Effectiveness is about whether a particular EU Action, in this case the existence of ENISA, has met its objectives and supporting tasks as set out in articles 2 and 3 of the Regulation, i.e. it is outcome focused. In response to the questions about effectiveness, the evaluation concluded that ENISA met its 5 objectives but not all to the same extent. In particular, the need to prioritize its activities according to the annual work programme set by the Management Board, led the Agency to focus its effort more on the needs of Member States and EU institutions than of the industry. In the same way, ENISA has achieved to a less extent the objectives linked to the development and maintenance of expertise and the support to policy development and implementation.

[15] Previous evaluations of ENISA in 2014 and in 2015 along with interviews in the current study affirmed that ENISA does not have sufficient outreach to industry and academia.

The evaluation concludes that ENISA has effectively created strong and trustful relationships with some of its stakeholders, notably with the Member States and the CSIRT community.

ENISA was most effective in strengthening capabilities, in particular in providing support to develop national CSIRTs, as also evidenced by responses to the survey of CSIRTs (see below), and national cybersecurity strategies[16]. Interventions in the area of capacity building were perceived as important in particular for less resourced Member States. Furthermore, the majority of Article 14 requests for assistance concerned Member States request for training supports[17]. The findings of the evaluation further suggest that the support provided by ENISA was perceived as complementary to that of other public interventions, clearly pointing out to a role for ENISA in the area.

Stimulating broad cooperation has been one of the highlights, with stakeholders widely agreeing on the positive role ENISA plays in bringing people together. The evaluation also concluded that there was comprehensive implementation of tasks supporting voluntary cooperation with stakeholders within the Union. In particular the Cyber Europe exercises[18], support to the CSIRT community, ENISA's publications and the European Cyber Security Month initiative are to be considered as key achievements. The Commission acknowledges that these specific initiatives are highly valued by Member States, CSIRTs and industry stakeholders.

It can be concluded that ENISA's activities have made an important contribution to **enhance cooperation** between Member States and related NIS stakeholders. This is further evidenced[19] by 82 of 88 respondents to a survey of ENISA direct stakeholders[20] asserting that ENISA had built strong and trustful relationships. This has further been confirmed by the results of the public consultation, where 79% of respondents affirmed that ENISA has achieved to some or great extent the objective of supporting cooperation in the cybersecurity community. Community building has been enhanced across Member States and in particular the cooperation between CSIRTs has increased.

As stated above, ENISA partially met the objective of providing **expertise**. Its guidelines and reports are used by many stakeholders but are more appreciated for their availability and the fact that they are coming from an EU Agency rather than for the outstanding quality of expertise. Some Member States (particularly those with significant cyber security capabilities[21]), some EU institutions and industry representatives would expect more from ENISA in terms of expertise. The findings show that ENISA struggles to hire experts, which can be explained by a combination of factors: the general difficulties across the public sector to compete with the private sector when trying to hire highly specialised experts; the low level of development of ENISA's human resources policies (HR department formally established only in 2016) and somewhat low level of

[16] In relation to national strategies, since 2013 ENISA has produced good practice guides on how to create and evaluate a strategy and it has run an experts group with the goal of information exchange on strategies lifecycle phases. It has furthermore directly supported 5 Member States in creating their strategy.

[17] 9 of the 13 Member States who made Article 14 requests for processing in 2015 involved training requests. Section 1.5.7. of the ENISA Annual Activity Report 2015 refers.

[18] ENISA developed a cyber-exercise capability that is able to train the EU cyber response teams to deal with crisis scenarios. Cyber Europe is the main cyber exercises of the European Union, engaging more than one thousand participants from the public and the private sector, taking place every 2 years since 2010.

[19] Supplemented by 51 of 65 respondents to the online public consultation.

[20] Management Board, Permanent Stakeholder Group

[21] ANSSI in France employs in excess of 600 people and over 700 staff are estimated in the UK's NCSC. .

attractiveness related to ENISA's location, for example linked to difficulties encountered by spouses to find work. As a consequence, ENISA heavily relied on the procurement of external expertise, involving 80% of its operational budget, in the implementation of tasks is a consequence.

All of this has to be balanced with the scope of ENISA's mandate as a horizontal Agency being very broad covering cyber security matters in energy, transport, finance, health, water, public administrations etc. The evaluation also found that ENISA provides an independent source of information and its capacity building role is highly valued by Member States, particularly by those with limited cyber security capacity.

ENISA has assisted the Member States and the Commission in developing and implementing the **policies** necessary to meet the legal and regulatory requirements of NIS.

The evaluation concluded that ENISA enhances cooperation and ensures capacity building but the development and maintenance of expertise and support of the development and implementation of policy is somehow limited. The key constraining factor is limited resources in an Agency with a very broad mandate and high expectations of its stakeholders. This is not a new situation, as a previous evaluation from 2007[22] recommended the Agency size should be increased to at least 100 staff. Moreover evaluations and impact assessments from 2009[23] and 2010[24] highlighted concerns about the Agency's ability to achieve planned impacts.

Efficiency

Summary: Despite its small budget – among the lowest compared to other EU agencies – the Agency has been able to contribute to targeted objectives, showing overall efficiency in the use of its resources. A location split between Athens and Heraklion required additional efforts of coordination and generating additional costs but the move to Athens in 2013 of the core operations department increased the agency's operational efficiency.

Efficiency is the extent to which outputs are maximised relative to inputs. Efficiency considers the relationship between the resources consumed by an intervention and the changes generated by it (which may be positive or negative). The assessment of the *efficiency* of ENISA considers the relationship between the resources used by the Agency and the output generated by its activities. Since this initiative does not present significant (direct, indirect, enforcement) regulatory costs, they have not been part of the assessment of ENISA efficiency.

ENISA ensures full budget execution and it demonstrates high efficiency in the implementation of its tasks as evidenced, among the others, by the volume of outputs. All deliverables planned in the annual work programmes were regularly executed. Statistics also show that downloads of publications have been consistent over the period under

[22] Communication from the Commission to the European Parliament and the Council on the evaluation of the European Network and Information Security Agency (ENISA) Brussels, 1.6.2007 COM(2007) 285 final

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

[24] SEC(2010)1126

review (approx. 900,000 downloads yearly), while the participants to the Cyber Europe exercise have increased from about 600 in 2014 to about 1000 in 2016.

The current governance structure is also considered as conducive to the efficient functioning of the Agency by 76 out of 88 respondents to the survey of the inner circle of ENISA stakeholders (Management Board, Executive Board etc.) but with more flexibility sought in the planning cycle. ENISA's working practices were found overall efficient by the external contractor. Some of the tools in place in the Agency are advanced in comparison to those used by other agencies and favour efficiency, for example the Agency's workflow paperless management system with the use of e-signatures.

The budget size forces the Agency to prioritise its work in undertaking the various tasks set out in its mandate. The Agency develops 50-60 publications every year, with approx. 900,000 downloads. As indicated above the Agency has indeed very limited resources: one of the smallest annual budgets (circa 10.4m€) and level of human resources (presently 84 staff) compared to 40 agencies covered by European Court of Auditors report[25] on agencies in 2016.

Almost all stakeholders agree that ENISA's resources are too low to implement all the given tasks. 38 of 54 respondents to the online public consultation expressed the view that the size of the Agency was inadequate. Under these conditions, ENISA has to prioritise its work to ensure resources are spent efficiently. At the same time, the Agency has to fulfil a number of administrative requirements as set by the Commission as an EU body. These requirements are the same for all EU agencies but weigh more heavily on smaller agencies due to significant fixed costs and inability to take advantage of economies of scale.

With regard to the Human Resources function, in 2015 ENISA spent 2.5% of its budget on staff recruitment, which is considerably higher than that in comparable Agencies in the benchmarking exercise. The focus on recruitment reflects the challenges of hiring and retaining cyber security professionals in challenging marketplace.

The set-up of an office in Athens (in 2013) to host the department of core operations contributed to efficiency gains, as it improved accessibility of the Agency. However, the split location of the Agency within Greece, with offices in both Athens and Heraklion means that ENISA has duplicate office accommodation costs and has to implement additional efforts to ensure coordination between the offices and bear the extra travel costs. In this context, its administrative expenditure is higher, at 14.8% of its budget, relative to other EU Agencies in the benchmarking exercise. In view of this situation no significant measures were identified to increase efficiency.

[25] By comparison, the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice - EU-LISA had a budget of 71.7m€ and 134 staff, Europol had a budget of 95m€ and 666 staff and the European Agency for the Management of Operational Cooperation at the External Borders – FRONTEX had a budget of 143.3m€ and 309 staff.

Relevance

Summary: In a context of technological developments and evolving threats and of significant need for increased network and information security (NIS) in the EU, ENISA's objectives proved to be relevant. In fact, Member States and EU bodies rely on technical expertise on the evolution of network and information security issues; capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. NIS continues to be a key political priority of the EU to which ENISA is expected to respond.

Relevance looks at the relationship between the needs and the problems in the society and the objectives of a given intervention.

In a context of technological developments and evolving threats and of significant need for increased network and information security (NIS) in the EU, ENISA's objectives proved to be relevant. Changes in the activities of ENISA based on the annual work programme show that the way the objectives have been defined allows for flexibility to focus on different needs from one year to another.

Most interviewees considered all of ENISA's objectives to be of continued relevance. Some stakeholders, including Member States wanted ENISA to have a role as an analytical centre, analyzing threats and incidents in detail to provide more informed advice while others sought further cooperation with Europol.

Direct stakeholders interviewed asserted that ENISA was well aligned with the priorities of the stakeholders, particularly with the NIS Directive and the Commission's communication from July 2016[26]. Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, assistance in the development of new policies on NIS is required and stakeholders need to cooperate.

Enhancing capabilities can be considered a highly relevant objective, in particular given the need for an agency to help less resourced Member States. This is also instrumental, in the context of increased cyber threats, to achieve higher degree of information sharing by ensuring the counter-parts have to some extent similar capacity levels.

Half of the respondents (31 of 62 responses) to the online public consultation considered all of ENISA's services, encompassing guidelines and recommendations, training materials and events, reports, the Cyber Europe Exercise, technical advice, events and Article 14 requests for assistance to be very relevant, relevant or somewhat relevant.

Community building followed by capacity building were the 2 key themes of most relevance to the different categories of stakeholders. It emerged that ENISA's key strength lays in brokering and facilitating cooperation between Member States and in particular the CSIRTs and is essential for delivery of EU political priorities.

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

In conclusion ENISA's objectives have been so far highly relevant in regard to cybersecurity matters. Cybersecurity is cross border in nature and impacts on the resilience of the Digital Single Market. On matters of digital privacy, stakeholders took the view that ENISA was not best suited to addressing it given the distinct interests and conflicts that can arise between digital privacy and cybersecurity.

Coherence

Summary: ENISA's activities have been generally coherent with the policies and activities of its stakeholders, at national and EU level, but there is a need for a more coordinated approach to cybersecurity at EU level. The potential for cooperation between ENISA and other EU bodies has not been fully utilised. The evolution in the EU legal and policy landscape make the current mandate less coherent today.

The evaluation concluded that ENISA's activities have been generally coherent with the policies and activities of its stakeholders but there is a need for a more coordinated approach to cyber security at EU level.

ENISA's activities have been coherent with the activities of the Member States. In particular, while ENISA itself is not a CSIRT, it provides training and networking support measures for the Member State based CSIRTs. There is a strong coherence between ENISA's activities and those of the national CSIRTs with respondents to the survey of CSIRTs highlighting ENISA's role in organising workshops and conferences and facilitating co-operation via the CSIRT Network.

Member States have very diverse stakeholder needs. Some Member States have well advanced capabilities in cybersecurity (for example encompassing national laws, strategies, funding, partnerships with the private sector and well-resourced public authorities with a dedicated cybersecurity remit, proactive CSIRTs) whereas others have very limited capabilities and resources (for example absence of laws, public bodies, funding, reactive CSIRTs etc). While there is some duplication of effort with respect to some Member States' national cyber security authorities (e.g. in terms of expertise, extent of preparedness etc) as set out in the positioning exercise, stakeholder interviews indicated that other Member States are in need of capacity building support and are reliant on ENISA.

The evaluation also concluded that ENISA activities were highly coherent with the policies at EU level. In particular, the evaluation found them in line with the objectives of the EU Cybersecurity Strategy, the NIS Directive and the security provisions of related policies, such as the ePrivacy Directive and the General Data Protection Regulation. Some of the activities performed by ENISA in the period under consideration, for example the pan-European cyber exercises and the European Cybersecurity Month campaign, were stemming from the Cybersecurity Strategy itself. Furthermore, in the course of 2016, ENISA has amended its annual work programme for that year in order to ensure coherence with the provisions of the NIS Directive.

At organisational level, ENISA activities were found to be coherent with those of the European Commission and other EU bodies. However the potential for cooperation between ENISA and the European Commission as well as other EU bodies is not fully utilised. There is general complementarity of the work between ENISA and the Joint

Research Centre (JRC) [27] of the Commission as the organisations vary in the stakeholders they target and approach issues from a different perspective. However, there is a risk of duplication of efforts as there is no systematic direct coordination (it mostly happen through the DG CONNECT).

Good levels of cooperation and coordination have been achieved between ENISA and EC3: little to no overlap was identified between the two organisations, which overall seem to cooperate well. However, there is room for more multilateral coordination to ensure better coherence and complementarity i.e. in the case of ENISA, EC3, CERT-EU and sectoral EU authorities who are developing competence in cyber, in order to attain increased NIS in Europe.

In particular, from the evaluation it emerged a risk of overlap between CERT-EU and ENISA with a risk of duplication of services to national CSIRTs. This would appear to be linked to direct support and assistance to Member States' CSIRTs and cross-border operational cooperation. CERT-EU is the computer emergency incident response team of the EU institutions and as a CSIRT it has peer to peer relationships with the Member State CSIRTs. ENISA is not a CSIRT but provides capacity building supports for CSIRTs.

EU Added Value

Summary: EU-added value: ENISA's added value lied primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related NIS communities. There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. The added value provided by the agency varied according to the diverging needs and resources of its stakeholders (e.g. big versus small Member States; Member States versus industry) and the need for the agency to prioritize its activities according to the work programme.

EU added value is about the benefits of initiatives taken at European level relative to solely national domestic approaches.

The evaluation found that ENISA added value primarily in enhancing cooperation, mainly between Member States but also with related NIS communities. This has been a key achievement in an area with a strong cross-border dimension. ENISA's activities could have been to some extent replaced nationally or through regional/bilateral cooperation but it would have been difficult to ensure the same community building across the Member States without a decentralised EU agency for cybersecurity. Prior to the establishment of ENISA, key initiatives such as the Cyber Europe exercises and CSIRT capacity and trust building with Member States did not exist. In absence of an EU agency, there may have been a reduced focus on cyber security by those Member States with fewer resources who, to date, have made very limited investments in cyber security capabilities.

[27] See https://ec.europa.eu/jrc/en/research-topic/cybersecurity

Highlights of ENISA's added value

Certification - as a neutral third party ENISA supports work related to establishing a possible EU ICT certification framework. It conducted consultation with more than 18 Member States, carried out an EU-wide survey on set of policy options and an analysis of EU certification laboratories landscape; ENISA also elaborated sector specific needs for ICT security certification (e.g. semiconductor industry). ENISA is regularly invited to participate in the Management Team meetings of the SOGIS group to offer policy advice to support the SOGIS Mutual Recognition Agreement (MRA).

ENISA Threat Landscape –an annual report providing an overview of threats, current and emerging trends to inform threat assessments and policy making became a reference point for cybersecurity community cited in a large number of prestigious sources and used as education material in universities and industry training courses.

ENISA has added value as facilitator for the essential trust building and cooperation between the various stakeholders (i.e. Member States, industry, users etc) in cyber security, through joint exercises such as Cyber Europe, is role as networking facilitator for Member State CSIRTs, provision of independent and neutral guidance and advice, the supports for policy implementation. These activities have positively impacted on the trust and confidence in the Digital Single Market. The evaluation found that while all categories from stakeholders – Member States, industry, research community – benefitted by an action at EU level, their needs have not equally been met due to the small size of the Agency compared to the challenge of bringing added value in such a vast field like cybersecurity.

Highlights of ENISA's added value

CSIRTs support: ENISA provides continuous capacity building support (2014 - 2017: 114 training courses, assistance under the Article 14 provided over 23 times). ENISA is the Secretariat for CSIRT Network established by the NIS Directive.

Cyber Europe Exercises – this largest and most comprehensive bi-annual EU cyber-security exercise has given the opportunity to around 4000 cybersecurity experts from over 2000 different organisations to be trained to deal with difficult and complex cybersecurity incidents. The level of satisfaction with the exercise is high to very high for over 99,9% of the participants.

European Cybersecurity Month (ECSM) – the cybersecurity awareness raising campaign running each year for the entire month of October mobilised so far over 30 countries all over Europe to organise activities, conduct media and social media relations.

The evaluation noted that most stakeholders think that in the future ENISA could take on a more important role in the EU cyber security landscape. This potential of the Agency would be lost in case of a discontinuation. According to some of the interviewees, the division of ENISA's activities across different organisations could lead to further fragmentation in the cyber security field in Europe as sector specific cyber security 'silos' of competence emerge. Such an approach would be at odds with increased importance of cyber security on the EU policy development agenda.

6. CONCLUSIONS

ENISA was entrusted with a broad mandate and its objectives proved to remain **relevant** today. In a context of technological developments and evolving threats and of significant need for increased network and information security (NIS) in the EU, there is a need for technical expertise on the evolution of network and information security issues.

Capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions.

Despite its small budget, the Agency has been operationally **efficient** in the use of its resources and implementation of its tasks. The location split between Athens and Heraklion, however, generated administrative costs.

In terms of **effectiveness,** ENISA partially met its objectives. The agency successfully contributed to increased NIS in Europe by offering capacity building in 28 Member States[28], enhancing cooperation between Member States and NIS stakeholders; provision of expertise, community building and support to policy. Overall, ENISA diligently focused on the implementation of its work programme and acted as trusted partner for its stakeholders in a field which only recently has been recognised to have such strong cross-border relevance. For long, cybersecurity has primarily been seen as an area of national competence, where EU intervention was only partially accepted.

ENISA managed to make an impact, at least to some extent, in the vast field of NIS but it has not fully succeeded in developing a strong brand name and gaining sufficient visibility to become recognised as a "the" centre of expertise in Europe. The explanation for this lies with the broad mandate of ENISA, which was not met with proportionally big resources. Furthermore, ENISA remains the only EU agency with a fixed-term mandate which limits its ability to develop a long term vision and support its stakeholders in a sustainable manner. This is also in contrast with the provisions of the NIS Directive, which entrust ENISA with tasks with no end date. Finally, the assessment found that this partial effectiveness can partly be explained to the high reliance on external expertise over in-house expertise, and the difficulties in recruiting and retaining specialised staff.

ENISA's **added value** lies primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related NIS communities (in particular between CSIRTs). There is no other actor at EU level that supports the cooperation of the same variety of stakeholders on NIS. However, due to the need to strictly prioritize its activities, ENISA's work programme is mostly guided by the needs of Member States. As a result, it does not sufficiently address the needs of other stakeholders, in particular the industry. It also made the Agency reactive to fulfilling the needs of its key stakeholders, preventing it from achieving a bigger impact. Therefore, the added value provided by the Agency varied according to the diverging needs of its stakeholders and the extent to which the Agency was able to respond to them (e.g. big versus small Member States; Member States versus industry).

Recommendations

The cybersecurity threat landscape is evolving fast with new threats emerging as Europe becomes ever more reliant on digital infrastructure and services through not only

28 Respondents to the public consultation were asked to comment on what they perceived as ENISA's main achievements over 2013-2016. Respondents from all groups (in total 55, including 13 from national authorities, 20 from private sector and 22 from "other") perceived the following as ENISA's main achievements: !) The coordination of the Cyber Europe exercises; 2) The provision of support to CERTs/CSIRTs through training and workshops fostering coordination and exchange; 3) ENISA's publications (guidelines and recommendations, threat landscape reports, strategies for incident reporting and crisis management etc.) that were considered as useful to create and update national security frameworks, as well as for reference to policy makers and cyber practitioners; 4) Assisting with the promotion of the NIS Directive; 5) Efforts to increase awareness on cybersecurity via the cybersecurity month.

connected devices but now omnipresent connectivity. The Internet of Things creates new opportunities related to energy efficiency, environmental protection, connected mobility, real time health monitoring and smart and seamless financial transactions in the digital economy and society. However in tandem with these business drivers are new vulnerabilities and exploits enabling compromised devices to disrupt the Digital Single Market.

Europe needs a focal point to address these new threats which are horizontal in nature impacting on multiple industrial sectors. The findings of this evaluation suggest that there could be a need for an EU Agency organised on a cross sectoral/horizontal basis with a strong mandate. The evaluation also found that there is also a need for cooperation and coordination across different stakeholders. The need for a coordinating entity at EU level to facilitate information flows, minimise gaps and avoid overlapping of roles and responsibilities becomes ever more acute. A decentralised EU agency and a neutral broker, could ensure a coordinated approach to cyber threats in the EU.

List of Annexes

Annex 1: Procedural Information

Annex 2: Stakeholder Consultation – See Annex 2 of Impact Assessment.

Annex 3: Evaluation questions

Annex 4: Contractor's Report – See Annex 6 of the Impact Assessment.

Annex 1: Procedural Information

Lead DG, Decide Planning

This evaluation Staff Working Document was prepared by Directorate H "Digital Society, Trust and Cybersecurity" of Directorate General "Communications Networks, Content and Technology".

The Agenda Planning reference of the initiative "Evaluation of the European Union Agency for Network and Information Security (ENISA), is 2017/CNECT/002.

Organisation and Timing

Several other services of the Commission with a policy interest in the assessment of the initiative have been associated in the development of this analysis.

An Inter-Service Steering Group (ISG), consisting of representatives from various Directorates-General of the Commission and the European External Action Service (EEAS), was set up in 2016 to steer the evaluation of ENISA during all key phases.

The ISG on the evaluation of ENISA met twice, on 24 June and 9 December 2016. DG CNECT, DG HOME, DG JRC, DG JUST, EEAS, and Secretariat General (SG) participated in the meetings. The Steering Group approved the evaluation roadmap, the terms of reference of the external study and the questionnaire of the public consultation. Further consultations, in particular with regard to the study, were carried out by written procedure.

The ISG was further expanded in the context of the review of ENISA and the set-up of an EU cybersecurity certification and labelling framework.

The Commission Directorate General for Communications Networks, Content & Technology (DG-CNECT) concluded a tender with a consortium led by CARSA[29], to provide an independent evaluation of ENISA in November 2016.

Evidence, Sources and Quality

The Commission gathered qualitative and quantitative evidence from various sources (a summary of which is attached to Annex 2 of the Impact Assessment report):

(1) Four weeks online public consultations regarding the evaluation and review of ENISA (19 January- 12 April 2017);

(2) A stakeholder workshops with Member States, industry and academia representatives;

(3) A study conducted by the above mentioned contractor;

(4) Fifty expert interviews conducted by the external contractor;

[29] Consortium includes CARSA (Consultores de Automatización y Robótica S.A. - lead partner), Logotech (partner), Ramboll Management Consulting S/A (partner), AIT Austrian Institute of Technology GmbH (partner), ZSI – Zentrum für Soziale Innovation (partner) and Agilis S.A. (partner).

(5) A survey on the ENISA review to the Computer Security Incident Response Teams Network;

(6) A survey to ENISA Management Board, Executive Board, Permanent Stakeholder Group, and ENISA staff;

(7) Direct dialogue with stakeholders;

(8) A roundtable with European Commission Vice-President for the Digital Single Market, Andrus Ansip, on 25 April 2017; and

(9) Desk research and literature review done in-house by DG CONNECT.

With regard to the quality of the evidence, the following points must be noted:

- There are limitations with regard to gathering data. For instance, the public consultation on the ENISA review received 90 submissions. With a total of 90 responses, the results of the public consultation cannot be considered to be fully representative of all stakeholders concerned. However, the views of national authorities of 15 Member States (including the position paper provided by France) are represented. The private sector is represented by 27 respondents which include eight umbrella organisations, thus representing a significant number of European enterprises whose activities are linked with cybersecurity;

- As regards the survey on ENISA, which was addressed to CERTs and CSIRTs, the answers in both surveys were anonymous. Thus, it is not possible to know whether some of the respondents might have started the survey and only partially completed and might have reopened it using a different browser or device and completed the survey then. This would result in answers that are double counted.

Annex 3: Evaluation questions

The evaluation roadmap set out the key questions to be addressed by the evaluation.

Effectiveness:

- To what extent has the Agency achieved its objectives and implemented the tasks set out in its mandate? What are the key factors influencing/restricting progress and how do they link to the agency (if at all)?
- What have been the benefits of acting at Agency level both from the operational and strategic perspective?
- To what extent has ENISA contributed to the overall EU goal of increasing network and information security in Europe?
- How appropriate is the balance of activities in relation to different cybersecurity and digital privacy topics considering the evolving needs of the main stakeholders?
- To what extent ENISA became an EU-wide centre of expertise and a reference point for EU institutions, Members States and the wider stakeholders community, in providing guidance, advice and assistance on issues related to network and information security?
- How effectively the Agency manages to set its work priorities?
- How effectively does the Agency tackle important upcoming, unplanned issues deriving by demands of its constituencies and/or EU policy priorities?
- Does the Agency consistently perform the same tasks with the same quality level over the time?
- How does ENISA compare to the other EU and national bodies offering similar services in relation to their capability to satisfy the cybersecurity and digital privacy needs of ENISA's constituency?
- To what extent has ENISA been more effective in achieving its results compared to other past, existing or alternative national or EU level arrangements?
- How do the current governance, the internal organisational structure and the human resources policies and practices of ENISA contribute to efficiencies and effectiveness in the work of the agency?
- How effective has ENISA been in building a strong and trustful relationship with its stakeholders when executing its mandate?
- What is the impact of the current arrangements related to the location of ENISA's offices on the overall capability of the Agency of meeting its objectives?

Efficiency:

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

- Were the annual budgets of the Agency implemented in an efficient way with a view on achieved results?

- Have the resources allocated to the agency been sufficient for the pursuing of its tasks (input/output analysis)?

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

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

- To what extent are the internal mechanisms for programming, monitoring, reporting and evaluating ENISA adequate for ensuring accountability and appropriate assessment of the overall performance of the Agency while minimising the administrative burden of the Agency and its stakeholders (established procedures, layers of hierarchy, division of work between teams or units, IT systems, etc)?

- To what extent has ENISA succeeded in building up the in-house capacities for handling various tasks entrusted to it? Are the "make or buy" choices made according to efficiency criteria?

- To what extent and how have external factors influenced the efficiency of ENISA?

Coherence:

- To what extent is ENISA acting in cooperation with the European Commission and other EU bodies, to ensure complementarity and avoid duplication of efforts?

- To what extent is ENISA acting in cooperation with the Member States to ensure complementarity and avoid duplication of efforts?

- To what extent are ENISA activities coherent with the strategy documents adopted in this policy field?

- Are the procedures put in place effective to ensure that ENISA's cooperation activities are coherent with the policies and activities of its stakeholders?

- What are the risks/sources of overlaps/conflict of interests?

Relevance and EU added value:

- What would be the most likely consequences at the EU level of stopping ENISA?
- How could ENISA increase its added value and its contribution towards the EU, the Member States and the private sector in the future, using the capabilities and competences already in place?
- How far are the Agency's tasks and resources aligned with key EU political priorities?
- Which Agency tasks are absolutely essential to deliver on these priorities?
- Which Agency tasks are necessary to continue implementing existing and evolving obligations under the Treaties and EU legislative framework?
- Are there some Agency tasks that have become redundant / negative priorities? If so, which are they?
- Are the objectives set out in the mandate of ENISA still appropriate given the current cybersecurity and digital privacy needs, regulatory and policy framework and needs?
- Have some of the initially non-core activities of the Agency become part of its core-business? What was the rationale in such cases?
- What would be the most likely consequences at the EU level of stopping ENISA's activities?

Other questions:

- Does the new scenario with increased frequency, sophistication and potential impact of cyber-threat trigger new needs from ENISA's constituency? To what extent could ENISA’s current mandate, tasks and/or capabilities address these needs?
- How does the new policy and regulatory landscape, having regard to the recently adopted Network and Information Security Directive and the priorities set by the Digital Single Market Strategy, impact on ENISA's activities?
- What are the main strengths and weaknesses of ENISA, within its current mandate and organisational set-up and capacity, in taking up the new challenges?
- Is a fixed-term mandate coherent with the new challenges and tasks ENISA will have to take on?

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

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

- How could ENISA's mission, tasks, working practices or activities be further developed in order to better respond to the new cybersecurity landscape?

- What would be the financial implications associated to each of the possible options for modifying the mandate as they emerge from the evaluation?

Annex4 : Contractor's Reports (See annex 5 of the Impact Assessment Report).

"*Study on the Evaluation of the European Union Agency for Network and Information Security*" by Ramboll and Carsa for the European Commission Directorate-General of Communications Networks, Content & Technology

"*Evaluation of ENISA Public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA) Synopsis report*" A study prepared for the European Commission DG Communications Networks, Content & Technology by Ramboll and Carsa.