EUROPEAN
COMMISSION

Brussels, 13.9.2017
SWD(2017) 500 final

PART 1/6

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT

Accompanying the document

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

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

{COM(2017) 477 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

Table of Contents

Table of Figures

Table of Tables

List of Annexes

Annex 1 Procedural Information, including organisation and timing of the initiative, exceptions to the Better Regulation Guidelines, the replies to the ISG comments made and the list of evidence provided.

Annex 2 Stakeholder Consultations, including the consultation strategy (which stakeholders, which type of mechanism) and the individual consultation results.

Annex 3 EU Agencies Budget and Staff, providing information on the total EU financial contribution to the 32 decentralised EU agencies, as well as their authorised establishment plans (i.e. staff) in 2017.

Annex 4 Preliminary Mapping of the 16 **EU-level Entities that Provide Cybersecurity Content.**

Annex 5 Final Study on the Evaluation of ENISA, as delivered 20 July, 2017 which involves an evaluation over the 2013-2016 period, assessing the Agency's performance, governance and organisational structure, and positioning with respect to other EU and national bodies. It assesses ENISA's strengths, weaknesses, opportunities and threats (SWOTs) with regard to the new cybersecurity and digital privacy landscape. It also provides options to modify the mandate of the Agency to better respond to new, emerging needs and assesses their financial implications.

Annex 6 Economic Analysis of Policy Options for ENISA, providing an estimation of the costs related to each of the four options for the future of ENISA derived from the results of the evaluation of ENISA.

Annex 7 ICT Security Certification Study as final version of the commissioned study providing the essential evidence base for the Impact Assessment, as delivered 25 July, 2017.

Annex 8 JRC Study on Certification, which investigates and proposes recommendations for the establishment of a European ICT security certification framework and assesses the feasibility of a European cybersecurity labelling framework.

Annex 9 Sectoral Mapping of EU and International initiatives on Cybersecurity, as recently revised which maps ongoing initiatives in the field of cybersecurity across key sectors covered by Chapter III of the NIS Directive: energy, transport, banking and finance, health, drinking water.

Annex 10 Who is Affected and How, describing the practical implications of the preferred option identified in the Impact Assessment for stakeholder groups likely to be directly or indirectly affected by the initiative.

Annex 11 ICT Security Certification Landscape, which lists the International and national certification schemes and other initiatives.

Annex 12 Case Studies as a new annex on certification schemes in the areas of smart meters, and cloud computing.

GLOSSARY

The below table explains the key terms or acronyms used in this document.

Term or acronym	*Meaning or definition*
2016 Council Conclusions	Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry – 15 November, 2016.
2016 Cybersecurity Communication	Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.
Accreditation	Accreditation means an attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity. (see also EC Reg. No. 765/2008)
ACER	Agency for the Cooperation of Energy Regulators.
ANSSI	Agence nationale de la sécurité des systèmes d'information; this is the National Cybersecurity Agency of France.
ARGUS	ARGUS is the Commission's general alert system in place since 2005. It is a process supported by an information technology (IT) tool and a dedicated network of 24/7 duty officers in each relevant Directorate-General
Blueprint	Framework (under preparation) for EU level approach on responding to large-scale cross-border cybersecurity incidents or cybersecurity crises.
BSI	Bundesamt für Sicherheit in der Informationstechnik; the German Federal Office for Information Security.
BSPA	The Dutch Baseline Security Product Assessment.
CAB	Conformity Assessment Bodies (please see below the definition).
C-ITS	Cooperative Intelligent Transport Systems.
CEF	Connecting Europe Facility.
Certification	The formal evaluation of products, services and processes by an independent and accredited body against a defined standard and the issuing of a certificate indicating conformance.
CERT(s)	Computer Emergency Response Team(s).
CERT-EU	This is a Computer Emergency Response Team CERT-EU for the EU institutions, agencies and bodies.

Term or acronym	*Meaning or definition*
CII(s)	Critical Information Infrastructure(s).
Common Approach on decentralised agencies	Joint Statement of the European Parliament, the Council of the European Union and the European Commission on decentralised agencies – Common Approach – 2012.
Common Criteria (CC)	The Common Criteria for Information Technology Security Evaluation (commonly known as CC) is an international standard (ISO/IEC 15408) for computer security evaluation. It is based on third party evaluation and envisages 7 evaluation assurance levels. The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that CC certificates are recognized by all the signatories of the CCRA.
Communication on the DSM Strategy Mid-term Review	Commission Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy – COM (2017) 228.
Conformity assessment	The process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.
Conformity assessment bodies	A body that performs conformity assessment activities including calibration, testing, certification and inspection.
CPA	Commercial Product Assurance.
cPPP	Contractual Public-Private Partnership on cybersecurity, signed by the European Commission and the European Cyber Security Organisation (ECSO) on 5 July 2016.
Critical infrastructure	'Critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (as defined by Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection).
CSIRT	Computer Security Incident Response Team.
CSPN	Certification Sécuritaire de Premier Niveau.
Cybersecurity	Cybersecurity comprises all activities necessary to protect network and information systems, their users and other impacted persons from cyber risks and threats.
Cyber Europe	ENISA manages the programme of pan-European exercises named Cyber Europe. This is a series of EU-level cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States.

Term or acronym	*Meaning or definition*
DSM Strategy	Commission Communication – A Digital Single Market Strategy for Europe – COM/2015/0192.
EAL	Evaluation Assurance Level.
EASA	European Aviation Safety Agency.
EC3	European Cybercrime Centre at Europol.
ECCB	European Cyber-certification Group proposed by Option 3 regarding certification.
ECSM	European Cyber Security Month.
ECSO	European Cybersecurity Organisation. It is an umbrella organisation whose members include a wide variety of stakeholders such as large companies, SMEs and start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.
EDA	European Defence Agency.
EEA	European Economic Area.
EECC	Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM/2016/0590 final - 2016/0288 (COD).
EFTA	European Free Trade Association.
eIDAS Regulation	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
ENISA	European Union Agency for Network and Information Security.
ENISA Regulation	Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.
EU Cybersecurity Strategy	Joint Communication of the European Commission and the European External Action Service: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN(2013).

Term or acronym	*Meaning or definition*
European Agenda on Security	Commission Communication – The European Agenda on Security COM(2015) 185.
Evaluation / Evaluation report	Evaluation is an assessment of the effectiveness, efficiency, coherence, relevance and EU added-value of one single EU intervention. The Roadmap informs about evaluation work and timing. An evaluation report (SWD) is prepared by the lead service and presents the findings and conclusions about the evaluation. The quality of major evaluation reports is checked by the Regulatory Scrutiny Board against the requirements of the relevant guidelines prior to publication and/or transmission to the Legislator as part of a formal report from the Commission.
Framework Directive for Electronic Communications	Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), as amended by Directive 2009/140/EC and Regulation 544/2009.
H2020	Horizon 2020.
IACS	Industrial automation control systems.
ICT(s)	Information and communications technologies.
ICT Security Certification	The various documents submitted in and with the Impact Assessment reflect different actors as well as different publication dates. Therefore, several terms are used which are largely inter-changeable. In this case, the terms 'cybersecurity certification' and 'security certification' have also been used frequently.
Impact	In an impact assessment process, the term impact describes all the changes which are expected to happen due to the implementation and application of a given policy option/intervention. Such impacts may occur over different timescales, affect different actors and be relevant at different scales (local, regional, national and EU). In an evaluation context, impact refers to the changes associated with a particular intervention which occur over the longer term.
Impact Assessment / Impact Assessment report	Impact Assessment is an integrated process to assess and to compare the merits of a range of policy options designed to address a well-defined problem. It is an aid to political decision making not a substitute for it. The Roadmap informs whether an impact assessment is planned or justifies why no impact assessment is carried out. An impact assessment report is a Staff Working Document (SWD) prepared by the lead service which presents the findings of the impact assessment process. It supports decision making inside of the Commission and is transmitted to the Legislator following adoption by the College of the relevant initiative. The quality of each IA report is checked by the Regulatory Scrutiny Board against the requirements of the relevant guidelines.

Term or acronym	*Meaning or definition*
Implementation	Implementation describes the process of making sure that the provisions of EU legislation can fully enter into application. For EU Directives, this is done via transposition of its requirements into national law, for other EU interventions such as Regulations or Decisions other measures may be necessary (e.g. in the case of Regulations, aligning other legislation that is not directly touched upon but affected indirectly by the Regulation with the definitions and requirement of the Regulation). Whilst EU legislation must be transposed correctly it must also be applied appropriately to deliver the desired policy objectives.
Incident	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.
Initiative	An initiative is a policy instrument prepared at EU level to address a specific problem or societal need. An impact assessment will assess options to inform the policy content of the initiative.
Intervention	Intervention is used as umbrella terms to describe a wide range of EU activities including: expenditure and non-expenditure measures, legislation, action plans, networks and agencies.
IPCR	Integrated Political Crisis Response
ISACs	Information Sharing and Analysis Centres.
JRC	Joint Research Centre.
MS(s)	Member State(s).
Network and information systems	Network and information systems (as defined by article 1 of Directive (EU) 2016/1148 – the "NIS Directive") mean: "(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance"
NIS	Network and information security.
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Term or acronym	*Meaning or definition*
PSD2 (Payment Service Directive 2)	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
PSG	Permanent Stakeholder Group of ENISA.
R&D	Research and Development.
R&I	Research and Innovation.
Ransomware	A ransomware is a type of malicious software that infects the computer systems of users and manipulates the infected system in a way that the victim cannot (partially or fully) use it and the data stored on it. The victim usually receives a request to pay a ransom to regain full access to system and files.
Security	All aspects related to defining, achieving, and maintaining data confidentiality, integrity, availability, accountability, authenticity, and reliability. A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way.
SME(s)	SME(s) is the abbreviation for micro, small and medium-sized enterprises (SMEs). SMEs are defined in Commission Recommendation 2003/361 as enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.
SOG-IS	Senior Officials Group – Information Systems Security.
SOG-IS MRA	Senior Officials Group – Information Systems Security Mutual Recognition Agreement of Information Technology Security Certificates.
Stakeholder	Stakeholder is any individual or entity impacted, addressed or otherwise concerned by an EU intervention.
Standardisation	A voluntary, multi-stakeholder process aiming to develop these technical specifications that respond to legal, business, or societal requirements. The parties involved in standardisation usually include enterprises, users, standards organizations and governments.
Threat	Any circumstance or event with the potential to adversely impact an asset, system or part thereof through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
TFEU	Treaty on the Functioning of the European Union.
Vulnerability	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable compromising the security of the computer system, network, application, or protocol involved.

1. INTRODUCTION: POLITICAL AND LEGAL CONTEXT

Since 2013, when the first EU Cybersecurity Strategy[1] was adopted and the Regulation (EU) No 526/2013 set out the current mandate and tasks for European Union Agency for Network and Information Security (ENISA), the challenges related to cybersecurity[2] have significantly evolved alongside with technology and market developments.

Since then, cybersecurity and cybercrime have been included in the Commission political priorities on the **Digital Single Market Strategy**[3] (DSM) and in the **European Agenda on Security**[4]**.** The EU agencies, in particular **ENISA** and the **European Cybercrime Center** (EC3) at Europol, have been in the frontline in terms of supporting the EU response to cybethreats, for example by providing information on the threat landscape, supporting Member States in building their capabilities and providing operational and analytical support to Member States' investigations.

Following up from the 2013 strategy, two cornerstones for European cybersecurity were adopted in 2016: the **Directive on security of network and information systems**[5], (the 'NIS Directive') and the **contractual public-private partnership on cybersecurity**[6] between the EU and the European Cybersecurity Organisation (ECSO)[7].

These developments are helping to further build-up the EU's cybersecurity resilience.

Box 1 – The Directive on Security of Network and Information Systems (NIS Directive)

Adopted in 2016, the NIS Directive aims at ensuring a high common level of cybersecurity in the EU. The Directive builds on three main pillars aiming to ensure:

1. Member States (MS) **preparedness** by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;

2. **Cooperation** among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks.

[1] Joint Communication of the European Commission and the European External Action Service: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013).

[2] Cybersecurity comprises all activities necessary to protect network and information systems, their users and other impacted persons from cyber risks and threats.

[3] Commission Communication - A Digital Single Market Strategy for Europe - COM/2015/0192

[4] Commission Communication - The European Agenda on Security COM(2015) 185

[5] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

[6] Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation - C(2016) 4400.

[7] ECSO is an umbrella organisation whose members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as MS's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries

3. A **culture of security** across sectors which are vital for our economy and society and moreover rely heavily on ICTs. Businesses that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. These sectors include **energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure**. Also key **digital service providers** (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive. Similar requirements already apply to telecom operators and internet service providers through the EU telecoms regulatory framework.

ENISA is expected to play an important role in the implementation of the NIS Directive. In particular, the Agency provides the secretariat to the CSIRT network, which is the cornerstone of operational cooperation, and it is also called to assist the Cooperation Group in the execution of its tasks. In addition, the Directive requires ENISA to assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practices.

Box 2 – The contractual public-private partnership on cybersecurity (cPPP)

The cPPP was one of the key initiatives announced in the 2015 Digital Single Market Strategy.

The partnership was signed on 5 July 2016 by the Commission and the European Cyber Security Organization (ECSO).

The goal of this partnership is to stimulate European competitiveness and help overcome cybersecurity market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cybersecurity products and solutions.

The initiative leverages EU, national, regional and private efforts and resources - including research and innovation funds - to increase investments in cybersecurity. The partnership is supported by EU funds coming from the Horizon 2020 Research and Innovation Framework Programme (H2020) with a total investment of up to €450 million until 2020.

Nevertheless, cyberattacks are increasing at an alarming pace. The latest example of a ransomware[8] cyber-attack in May 2017 shows the potentially massive impact of a cyber-attack across sectors and countries: more than 150 countries and over 230,000 systems were affected, including those related to essential services such as hospitals, despite the damage being contained this time in comparison to the potential (deeper) consequences it may have had[9]. This example is just the last of a series: more than 4,000 ransomware attacks have occurred every day since the beginning of 2016, a 300% increase over 2015[10].

[8] A ransomware is a type of malicious software that infects the computer systems of users and manipulates the infected system in a way that the victim cannot (partially or fully) use it and the data stored on it. The victim usually receives a request to pay a ransom to regain full access to system and files.

[9] WannaCry Ransomware Outburst, Infonotes, ENISA, 2017 https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst.

[10] How to protect your networks from ransomware, CCIPS, 2016 https://www.justice.gov/criminal-ccips/file/872771/download.

The number and size of cyberattacks can affect public trust in the capacity of modern societies to ensure security and privacy, therefore undermining the very foundations of the digital economy. Moreover, the digital society is shifting from specific connected devices (computers, smartphones or wearables) to omnipresent connectivity (household items, industrial goods, etc.). By 2020 it is estimated that billions of devices, including consumer ones (televisions, refrigerators, washing machines etc.), will be connected to the internet in the EU alone.[11] A connected economy and society is more vulnerable to cyber threats and attacks and requires stronger defences.

In order to gain and preserve trust and security, ICT products and services need to incorporate security features directly in the early stages of their technical design and development. Customers and users need to be able to ascertain the level of security assurance of the products and services they procure or purchase. By providing specific procedures for the evaluation of security properties, formal processes such as certification play an important role in increasing trust and security in products and services. This is particularly relevant for new systems that make extensive use of digital technologies and which require a high level of security, such as connected and automated cars, electronic health, industrial automation control systems (IACS)[12] or smart grids.

Against this background, in the **2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry**[13], the Commission encouraged Member States to make the utmost use of the voluntary cooperation schemes under the NIS Directive. The Commission announced a number of measures to further step-up cooperation mechanisms and information and knowledge sharing to increase the EU's resilience and preparedness, also taking into account large scale incidents and a possible pan-European cybersecurity crisis. In this context, the Commission announced that it would advance the **evaluation** and **review** of ENISA as an opportunity for a possible enhancement of the Agency's capabilities and capacities to support Member States in a sustainable manner in achieving cybersecurity resilience.

Box 3 – The European Union Agency for Network and Information Security (ENISA)

ENISA was set up in 2004[14] to contribute to the overall goal of ensuring a high level of network and information security within the EU. In 2013, the Regulation (EU) No 526/2013 established the new mandate of the Agency for a period of seven years, until 2020. The Commission is required to conduct an evaluation of the Agency by 20 June, 2018 and address the possible need to modify its mandate and the financial implications of any such modification.

ENISA supports the European Institutions, the Member States and the business community in

[11] IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, study for the European Commission.

[12] DG JRC has published a report that proposes an initial set of common European requirements and broad guidelines related to cybersecurity certification of IACS components. Available at: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[13] Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.

[14] Regulation (EC) n° 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77, 13.3.2004, p. 1.

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[15]:

- **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 pan-European cyber exercises).
- **Enabling** (e.g. engagement with the stakeholders and international relations).

In the course of the negotiations of the NIS Directive, the EU co-legislators decided to attribute important roles to ENISA in the implementation of the law[16]. As an example of the spirit of the law, recital 38 strongly links ENISA to the Cooperation Group, stating that "the respective tasks of the Cooperation Group and of ENISA are interdependent and complementary".

ENISA has its offices in Greece, the administrative seat in Heraklion (Crete) and the core operations in Athens.

In the same Communication, the Commission noted that multiple national initiatives are emerging to set high-level cybersecurity requirements for ICT components on traditional infrastructure, including certification requirements. Even if important, these initiatives bear the risk of creating single market fragmentation and interoperability issues. Accordingly, the Commission announced that it would work, among others, on a **possible European ICT security certification framework proposal**, to be presented by end-2017, and to assess the feasibility and impact of a European lightweight cybersecurity labelling framework.

This vision was further confirmed in the 2016 **Council Conclusions**, which acknowledged that "cyber threats and vulnerabilities continue to evolve and intensify which will require continued and closer cooperation, especially in handling large-scale cross-border cybersecurity incidents". The conclusions reaffirmed that "the ENISA Regulation is one if the core elements of an EU cyber resilience framework"[17]. At the same time, the Council called on the Commission "to explore the opportunity to create a cybersecurity certification scheme, while reflecting the existing effective security schemes, if relevant, with a view to proposing measures, including legislative ones".

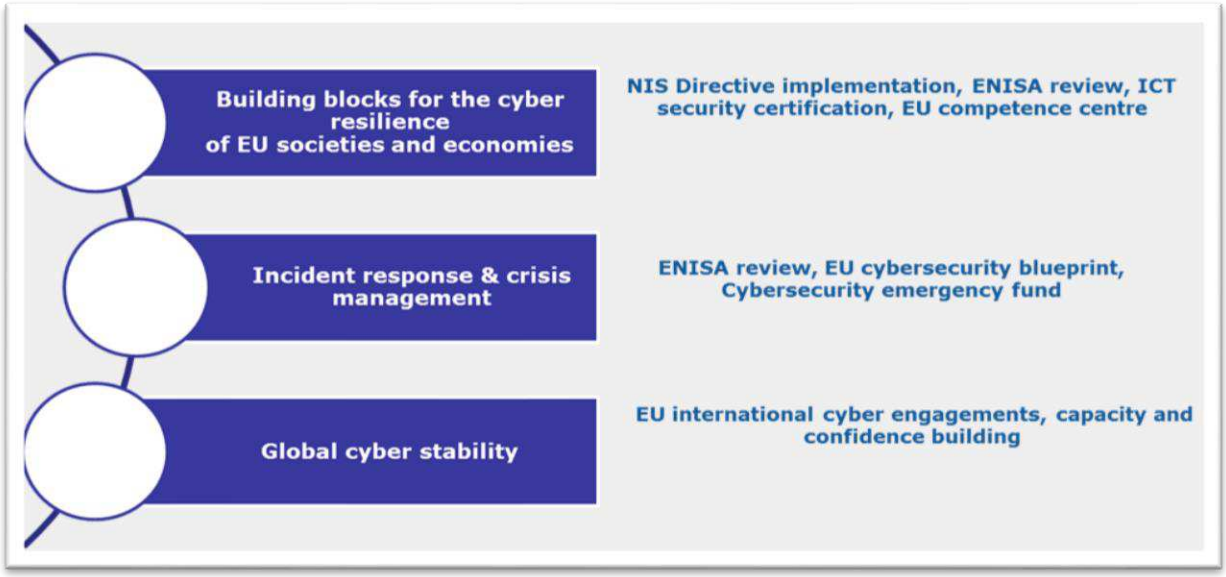
In its Communication on the **DSM Strategy Mid-term Review of May 2017**, the Commission further specified that by September 2017 it would review the 2013 EU Cybersecurity Strategy to address the risks faced today, help improve the security in the Union and Member States and increase the confidence and trust of businesses and people in the digital economy and society. Moreover, it would review the mandate of ENISA in order to define its role in the changed cybersecurity ecosystem and develop measures on

[15] https://www.enisa.europa.eu/publications/corporate/enisa-strategy
[16] See in particular articles 7, 9, 11, 12, 19 as well as recitals 36, 68 and 69 of Directive (EU) 2016/1148.
[17] Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

cybersecurity standards and certification to make ICT-based systems, including connected objects more cyber-secure.[18] This approach has been endorsed by the **European Council** in June 2017, which welcomed the Commission's intention to review the Cybersecurity Strategy in September and to propose further targeted actions[19].

On this basis, the Commission is discussing a set of measures in three interrelated areas (see figure 1) as part of the Strategy's review that will be presented in the upcoming September Communication[20], which sets out the vision for the EU to adopt a proactive approach to protect European prosperity, society and values through effective cybersecurity. The Communication includes actions directed to increase EU resilience, step-up response to cyber attacks, stimulate a single market for cybersecurity and cooperate globally on cybersecurity and defence.

Figure 1 Priority areas for EU action in cybersecurity



The initiative under assessment in this report refers specifically to the review of ENISA and the policy on ICT security certification, which are combined as they address complementary aspects forming part of the overall effort to increase harmonisation of cybersecurity policy and ensure the proper functioning of the single market. In addition, the combined analysis of policies and organisational solutions to implement these with a view of developing a single legislative proposal is a common practice at EU level. One relevant example is provided by the Regulation establishing the European Aviation Safety Agency (EASA) which at the same time covers the common rules in the field of civil aviation[21]. In the case of the policy on ICT security certification, ENISA has been

[18] Commission Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy - COM(2017) 228.
[19] European Council meeting (22 and 23 June 2017) – Conclusions EUCO 8/17.
[20] JOIN(2017) 450

[21] Recital 12 of Regulation (EC) No 216/2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency: "There is a need for better arrangements in all the fields covered by this Regulation so that certain tasks currently performed at Community or national level should be carried out by a single specialised expert body. There is, therefore, a need within the

identified as the main organisation to support its implementation by virtue of ENISA being the only EU-level body with extensive experience and knowledge base in the field of security certification such as its Cloud Certification Schemes Metaframework (CCSM)[22] and standardisation (more details are provided in section 5.3). It can moreover present an organizational structure which ensures relevant, consistent and structured Member State input while mainitaining an independent EU-level verification capacity. Bringing cybersecurity resilience and cybersecurity certfication under one roof and under one Regulation would further favour efficiency gains and avoid the setting up of completely new organisational structures.

The proposed actions addressed in the present impact assessment would be part of the EU's wider resilience building efforts to be endorsed in the 2017 September Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'[23], and therefore also effect the work of ENISA. More specifically, in addition to addressing the end of the Agency's current mandate and the review of its tasks and functions, the proposed Regulation would also address the role of such an Agency in the wider cybersecurity ecosystem in the EU. Building on the responsibilities conferred to ENISA by the NIS Directive, this would include its role in in handling incidents for which Member States may ask ENISA for assistance and in large scale cross-border incidents referred to in the EU cybersecurity blueprint[24], an initiative that is part of the September 2017 Communication[25], which describes how national and Union actors should interact (cooperate and exchange information) in response to large scale cross-border cybersecurity incidents and crises within existing crisis management mechanisms such as the IPCR and ARGUS. The crisis management ecosystem as regards cybersecurity at Union level involves many actors including ENISA, CSIRTs Network, the European Cybercrime Centre (EC3) at Europol, and CERT-EU. As regards ENISA, blueprint it identifies its role and responsibilities within established crisis management procedures as well as the role it plays in the CSIRTs Network during crises.

The new Regulation would also build such a capacity that would allow ENISA to also have a role in providing assistance upon creation of an EU emergency fund[26] subject to the relevant legal instrument's requirements. ENISA's role would also be further enhanced and supported by the eventual creation of the European Cybersecurity Research

---

Community's existing institutional structure and balance of powers to establish a European Aviation Safety Agency (hereinafter referred to as the Agency) which is independent in relation to technical matters and has legal, administrative and financial autonomy. To that end, it is necessary and appropriate that it should be a Community body having legal personality and exercising the implementing powers which are conferred on it by this Regulation".

[22] See under: https://resilience.enisa.europa.eu/cloud-computing-certification

[23] JOIN(2017) 450

[24] In the COMM/2016/0410, the Commission announced that it would submit for consideration a cooperation blueprint to handle large-scale cyber incidents.

[25] JOIN(2017) 450

[26] The EU Cybersecurity Emergency Fund is an initiative developed in the context of the review of the Cybersecurity Strategy on the example of existing crisis mechanisms in other EU policy areas. It will provide the possibility for Member States to seek help at the EU level in case of major incident. It could be used to support, directly or indirectly, citizens, companies or public administrations hit by cyberattacks, provided that a basic level of cybersecurity protection had been in place before the incident occurred.

and Competence Centre[27], bringing together a network of European centres from which ENISA could draw further competences and expertise for its functions.

2. PROBLEM DEFINITION

2.1. Overview of the findings of the evaluation of ENISA and the relevant public consultations

The present impact assessment is supported, among other sources of evidence, by the results of the ex-post evaluation of ENISA (2013-2016 period) and two public consultations related to the evaluation and review of ENISA's mandate and the contractual public-private partnership (cPPP) on cybersecurity, where a section was devoted to the topic of ICT security certification. In this paragraph a brief overview of their results is presented, while a detailed summary can be found in Annex 2, together with the results of the targeted consultation activities. References to specific results are also included throughout the document.

The evaluation of ENISA

The Commission, according to the evaluation roadmap[28], assessed the **relevance, impact, effectiveness, efficiency, coherence and EU added value** of the Agency with regard to its performance, governance, internal organisational structure and working practices in the period 2013-2016. Inter alia, the results of stakeholder consultations for this evaluation suggest that ENISA's resources and mandate need to be adapted so that it can adequately support Member States to respond to the challenges of the future.

The main findings can be summarised as follows (for more see the Staff Working Document on the subject, accompanying the impact assessment).

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

Relevance: In a context of technological developments and evolving threats and of significant need for increased network and information security (NIS) in the EU,

[27] The European Cybersecurity Research and Competence Centre is an initiative developed in the context of the review of the Cybersecurity Strategy. Building on the work of Member States and the Public-Private Partnership, the Centre would be the central hub of a EU network of competence centres in Member States, This network and its Centre would stimulate development and deployment of technology in cybersecurity, implementing advanced cybersecurity research and adding a central capability that provides all of Europe with latest technologies and competences. The Centre will coordinate efforts in the area of research, training and marketing, addressing civilian, industrial, government and military needs promoting innovation and industrial competitiveness.

[28] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

ENISA's objectives proved to be relevant. In fact, Member States and EU bodies rely on expertise on the evolution of NIS, capacities need to be built in the Member States to understand and respond to threats, and stakeholders need to cooperate across thematic fields and across institutions. NIS continues to be a key political priority of the EU to which ENISA is expected to respond; however, ENISA's design as EU agency with a fixed-term mandate: (i) does not allow for long-term planning and sustainable support to Member States and EU Institutions; (ii) may lead to a legal vacuum as the provisions of the NIS Directive entrusting ENISA with tasks are of a permanent nature[29]; (iii) lacks coherence with a vision linking ENISA to an enhanced EU cybersecurity ecosystem.

Effectiveness: 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. The evaluation concluded that ENISA has effectively created strong and trustful relationships with some of its stakeholders, notably with the Member States and the CSIRT community, "acting as a neutral, independent broker at EU level and as a bridge between the strategic and operational worlds"[30]. Interventions in the area of capacity building were perceived as effective in particular for less resourced Member States. Stimulating broad cooperation has been one of the highlights, with stakeholders widely agreeing on the positive role ENISA plays in bringing people together. 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 very broad mandate. The evaluation also concluded that ENISA partially met the objective of providing expertise, linked to the problems in recruiting experts (see also below in the efficiency section).

Efficiency: Despite its small budget the Agency has been able to contribute to targeted objectives, showing overall efficiency in the use of its resources. The evaluation concluded that processes generally were efficient and a clear delineation of responsibilities within the organisation led to a good execution of the work. One of the main challenges to the Agency's efficiency relates to ENISA's difficulties in recruiting and retaining highly qualified experts. The findings show that this can be explained by a combination of factors, including the general difficulties across the public sector to compete with the private sector when trying to hire highly specialised experts, the type of contracts (fixed term) that the Agency could mostly offer and the somewhat low level of attractiveness related to ENISA's location, for example linked to difficulties encountered by spouses to find work. 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.

Coherence: 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.

[29] Reference to articles 7, 9, 11, 12, 19 of the Directive on Security of Network and Information Systems (NIS Directive).

[30] Study, Annex 5, p. 40

EU-added value: ENISA's added value lie primarily in the Agency's ability to enhance cooperation, mainly between Member States but also with related NIS communities. Indeed, "ENISA is providing significant added value to the cybersecurity activities implemented in the Member States"[31] 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. The evaluation concluded that a potential discontinuation of ENISA would be a lost opportunity for all Member States. It will not be possible to ensure the same degree of community building and cooperation across the Member States in the field of cybersecurity without a decentralised EU agency the picture would be more fragmented where bilateral or regional cooperation stepped in to fill a void left by ENISA.

Results of the public consultations on the contractual public-private partnership on cybersecurity (cPPP) and the ENISA evaluation and review.

The results from the 2016 consultation on cybersecurity cPPP[32] on the section on certification show that:

- 50,4% (e.g. 121 out of 240) of respondents do not know whether national certification schemes are mutually recognised across EU Member States. 25.8% (62 out of 240) replied 'No', while 23.8% (57 out of 240) replied 'Yes'.

- 37,9% of respondents (91 out of 240) think that existing certification schemes do not support the needs of Europe's industry. On the other hand, 17, 5% (42 out of 240) – mainly global companies operating on the European market - expressed the opposite view.

- 49.6% (119 out of 240) of respondents says that it is not easy to demonstrate equivalence between standards, certification schemes, and labels. 37.9% (91 out of 240) replied 'I do not know', while only 12,5% (30 out of 240) replied 'Yes'.

In addition, in the context of the 2017 public consultation on the evaluation and review of ENISA, 67.5 % of respondents to the specific question (54 out of 80, of which 11 national authorities) expressed the view that ENISA could play a role in establishing a harmonized framework for security certification of ICT products and services In terms of stakeholder coverage, the consultation provided a good and representative level of qualified input, covering relevant stakeholders ranging from operators of critical infrastructures, service providers, ICT vendors, associations from the ICT, banking or telecommunications sectors, to Member States and their cybersecurity and certification agencies. Their responses showed that stakeholders count on ENISA to continue its work and strengthen its role in the future. Some of the most supportive comments speak of it 'becoming a central information hub', 'a more visible agency in the service of all Member States', express the wish to 'confirm and reinforce' ENISA. Other comments highlight the need for ENISA to adapt to changing circumstances, also strengthening its

[31] Study, Annex 5, p. 92

[32] 240 stakeholders from national public administrations, large businesses, SMEs, microbusinesses and research bodies responded to the section on certification.

resources, or by offering 'real-time cybersecurity warnings' or commending the organisation of the cyber-exercises and acting as 'energizer for the industry' and 'enabler of a security designed in Europe label'. With specific regard to ENISA past performances and future, the main trends emerging from the 2017 consultation are the following[33]:

- The overall performance of ENISA during the period 2013 to 2016 was positively assessed by a majority of respondents (74%). A majority of respondents furthermore considered ENISA to be achieving its different objectives (at least 63% for each of the objectives). ENISA's services and products are regularly (monthly or more often) used by almost half of the respondents (46%) and are appreciated for the fact that they stem from an EU-level body (83%) and for their quality (62%).

- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU, in particular the top five (in a list of 16) were: cooperation across Member States; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation across Member States in matters related to cyber security; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks.

- A large majority (88%) of respondents considered the current instruments and mechanisms available at EU level to be insufficient or only partially adequate to address these. A large majority of respondents (98%) saw a need for an EU body to respond to these needs and among them ENISA was considered to be the right organisation to do so by 99%.

2.2. What is the size of the problems?

Europeans increasingly value and rely on digital technologies. According to a recent Eurobarometer survey[34], the majority of citizens think digital technologies have a positive impact on the economy (75%), on their quality of life (67%) and on society (64%).

Critical economic sectors such as transport, energy, health or finance have become increasingly dependent on network and information systems to run their core businesses. The Internet of Things (IoT), interconnecting objects between them and with people

[33] 90 stakeholders from 19 MSs replied to the consultation (88 responses and 2 position papers), including national authorities from 15 MSs, including France, Italy, Ireland and Greece, and 8 umbrella organisations representing a significant number of European organisations, for example the European Banking Federation, Digital Europe (representing the digital technology industry in Europe), European Telecommunications Network Operators' Association (ETNO). The ENISA public consultation was complemented by several other sources, including; (i) in-depth interviews, with approximatively 50 key players in the cybersecurity community; (ii) survey to the CSIRT Network; (iii) survey to the ENISA Management Board, Executive Board, Permanent Stakeholder Group.

[34] Attitudes towards the impact of digitisation and automation on daily life, Eurobarometer, 2017.

through communication networks[35], is already a reality and it is expected to boom in the near future: a few billions of IoT connections are forecasted in the EU in 2020[36].

While the growing digital connectivity brings enormous opportunities, it also exposes the economy and society to cyber threats.

Cyber-attacks are constantly on the rise. In some Member States, it has been estimated that half of all the crimes are cybercrimes[37]. Some of these attacks have aimed at high-profile targets, including power grids, important webmail services, central banks, telecommunications companies and electoral commissions. This is reflected also in citizens' own perception of risk: 86% of respondents to the latest Eurobarometer on the subject believe that the risk of becoming a victim of cybercrime is increasing[38].

A 2016 study by PwC revealed that the number of security incidents across all industries rose by 38% in 2015, which is the biggest increase in the past 12 years, while at least 80% of European companies have experienced at least one cybersecurity incident.[39]. In Q3 2016 alone, 18 million new malware samples were captured, i.e. an average of 200,000 per day.

Moreover, a large share of cybersecurity incidents are due to technical failures without malicious intent – deriving from products which are weak on security, to the lack of software updates or appropriate procedures – or are due to some type of human error.

Cyber incidents cause major economic damage to European businesses, undermine the trust of citizens and enterprises in the digital society and affect citizens' fundamental rights. A 2014 study[40] estimated that the economic impact of cybercrime in the Union amouted to 0.41% of EU GDP (i.e. around EUR 55 billion) in 2013; with Germany being the most affected Member States (1.6 % of GDP). A recent report, in the afternmath of the "wannacry" attack, estimated that a serious cyber-attack could cost the global economy more than $120bn (£92bn) – as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy[41].

The most affected sectors are financial services, energy, technology, services, industry and defence[42] and, as shown in figure 2, several big attacks to critical sectors were reported in 2016.

---

[35] Many IoT devices are either already available or are being developed for deployment in the near future, including: sensors to better understand patterns of daily life and monitor health; monitors and controls for home functions, from locks to heating and water systems; devices and appliances that anticipate a consumer's needs and can take action to address them (e.g., devices that monitor inventory and automatically re-order products for a consumer).

[36] Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, IDC and TXT, study carried out for the European Commission, 2014.

[37] PWC, Global State of Information Security Survey, 2016.

[38] Special Eurobarometer 464, 2017.

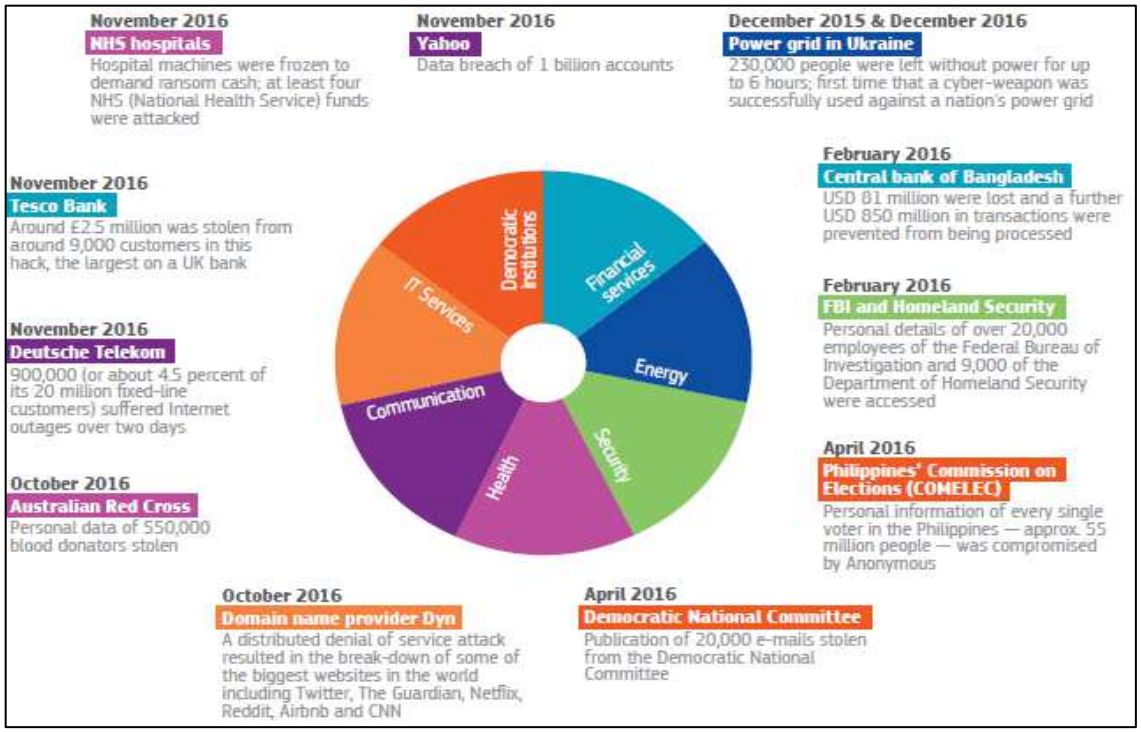
[39] PWC, Global State of Information Security Survey, 2016 and http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/

[40] McAfee & Center for Strategic and International Studies, 'Net Losses: Estimating the Global Cost of Cybercrime', 2014

[41] Counting the cost – Cyber exposure decoded, Lloyd's and Cyence, 2017.

[42] 2015 Cost of Cyber Crime Study: Global, Ponemon Institute October 2015.

Figure 2 Selection of significant cyber-attacks in 2016.



Source: European Political Strategy Centre, 2017

The IoT has brought new risks. This applies in particular to consumer IoT, as it can involve "non-technical" or "uninterested" consumers, who connect an increasingly wide variety of devices to their home networks. They risk losing track of which devices are connected to the Internet over time, therefore making the efforts of securing them even more challenging[43]. Connectable home devices, such as TVs, home thermostats or home alarms, create multiple connection points for hackers to gain entry into IoT ecosystems, access customer information, or even penetrate manufacturers' back-end systems[44].

Cyber threats evolve so rapidly that strategies and tools to prevent and respond to them easily become outdated. For example, in the public consultation on ENISA review, 83% of respondents considered that the current instruments and mechanisms at European level (such as the regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) are either "partially" or only "marginally adequate" and 5% found them "not at all adequate" to promote and ensure cybersecurity.

In this context, ICT security certification is a valuable tool whose use is inadequate in the EU. All participants to a recent ENISA survey (see Annex 2) agreed on the need to leverage on certification to mitigate cybersecurity risks. In addition, 40 out of 46

[43] Internet of Things (IoT) Security and Privacy Recommendations, Broadband Internet Technical Advisory Group Report, 2016. Risks of IoT are linked, among the others, to: lack of IoT supply chain experience with security and privacy; lack of incentives to develop and deploy updates after the initial sale; difficulty of secure over-the-network software updates; devices with constrained or limited hardware resources (precluding certain basic or "common-sense" security measures); devices with constrained or limited user-interfaces (which if present, may have only minimal functionality), and devices with malware inserted during the manufacturing process. Internet of Things (IoT) Security and Privacy Recommendations

[44] Cyber risk in an Internet of Things world, Flashpoint Report, Deloitte, 2015.

respondents[45] to a survey aimed at SMEs think that ICT security certification is a valuable tool to reduce cyber vulnerabilities of ICT products or services (see Annex 2).

2.3. What are the problem drivers?

The analysis of the evidence supporting the impact assessment identified the following main drivers contributing to the problem:

- Incomplete regulatory framework, in particular as regards a coherent approach to cybersecurity policies at the EU-level. Several pieces of legislation contain provisions on cybersecurity requirements, primarily; the NIS Directive, the General Data Protection Regulation (GDPR), the current Telecoms Framework (and the related proposal for a European Electronic Communications Code), the Payment Service Directive 2 (PSD2) but also market regulation (e.g. Radio Equipment Directive). These legislative acts do not provide for an EU-wide coordinated approach on the implementation of the requirements and the guidance on the implementation is entrusted to different agencies or bodies, risking a silo-ed and in many cases sectoral approach[46]. This leads to fragmentation of policies and approaches across Member States and EU institutions and agencies in an area where a harmonised approach is fundamental to increase resilience and ensure the functioning of the internal market.

- Immature cooperation mechanisms. Cooperation across Member States, between public and private actors and between the national and the EU level is taking shape, although at slow pace. In particular, the NIS Directive provides for mechanisms that can stimulate cross-border cooperation at least on a voluntary basis. However, these measures are only starting to take place. Furthermore, the shift in culture towards cooperation in an area close to national security takes time to progress especially at EU level, where cooperation takes place mostly on an ad-hoc basis or according to bilateral agreements between different actors. The low degree of development of cooperation mechanisms has a direct impact on the fragmentation of the policies and the approaches to cybersecurity across Member States and across the EU institutions, agencies and bodies.

- Lack of EU-wide reliable data and analyses. There is little information and independent analyses on key cybersecurity issues (such as the economics of cybersecurity, reliable trends of expected new challenges, the best solutions to face threats or criminal statistics related to cybercrime[47]) covering the whole EU. This applies in particular to the cybersecurity incidents. The incident reporting requirements of the GDPR, the NIS Directive and as well as other similar requirements stemming from other pieces of legislation[48], should somehow

[45] 4 replied "no", 2 replied "don't know"

[46] For example in the PSD2 it is the European Banking Authority, in the GDPR the Data Protection Board in the Telecoms Framework it is ENISA, in energy sector ACER, in aviation EASA etc.

[47] Article 14 of the Directive on attacks against information systems (2013/40/EU) requires the collection of statistics on the offences described in the Directive, and their transmission to the Commission. In 2015, the Commission published the results of an exploratory data collection on criminal statistics on cyber-attacks (based on the offences covered in the Directive on attacks against information systems): http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=21219&no=6

[48] For example, the PSD2, the Regulation on electronic identification and trust services for electronic transactions in the internal market - eIDAS, the recent proposal from a European Electronic Communications Code.

improve the situation, but primarily at the national level as notifications are to be addressed to the national authorities. This is insufficient for the EU needs and it leads to fragmentation of policies and approaches across the Member States and EU institutions, and to insufficient awareness and information of citizens and companies. In particular, companies that are present in more than one Member State, EU-level regulators or even national regulators in sectors with significant cross-border dependencies, need to be aware of the situation in the entire EU if they want to make reliable risk-based decisions or take appropriate measures. The lack of EU-wide reliable data also impacts the cybersecurity industry's ability to design products that would meet the requirements of companies and citizens across the whole EU.

- Limited efficiency and suitability of current certification mechanisms: The main mutual recognition instrument in Europe - the SOG-IS MRA - has a number of shortcomings.It only includes twelve Member States plus Norway and has developed only a few protection profiles regarding certain digital products (such as digital signatures, digital tachograph and smart cards). Furthermore, SOG-IS MRA is based on the methodology of Common Criteria (CC), which is criticised for the long duration of process and high costs, among others[49]. CC envisages seven Evaluation Assurance Levels (EAL), with one being the lowest-level evaluation and seven being the highest-level one[50]. It has been estimated that a CC certificate for the lowest level of assurance can be obtained in about six months at a cost of around EUR 20,000. A higher assurance level certificate (e.g. EAL 4) for an ICT product can take one to two years, and, often, by the time the process is completed a new version of that product is already delivered[51]. According to the smart metering industry, CC certification is the most expensive (not less than EUR 500,000) among the various certifications they have to provide. Govenments and industry have taken actions to develop more agile certification scheme. However, the use of these schemes is occurring in an uncoordinated way. As a result, manufacturers of products such as smart meters would typically need to apply for different certification schemes or comply with different security requirements across the EU. The duration of each certification process for these products can take from six months to one year. These initiatives acknowledge the importance of ICT security certification and are in line with the objective of mainstreaming cybersecurity in the EU policy making. However, they can also lead to dispersed resources and diverging approaches to cybersecurity if the initiatives across different policy domains are not, as it it currently the case, sufficiently coordinated.

- Insufficient and uneven resources allocated at national and EU level, is a driver for all three problems outlined in figure 3. Only in recent years has cybersecurity acquired a status of important policy where both governments and companies have decided to invest and yet, as presented above, it is still very difficult to estimate the return on such investments, sometimes making the choice to allocate resources difficult. The differences in the resources available across organisations, Member States and EU institutions impact directly the level of capabilities and preparedness of Member States, the EU capacity to complement

[49] For a description of criticism to CC, see pp 24-26 of the JRC study (Annex 8).
[50] An EAL defines how thoroughly the product is tested.
[51] http://www.eurecom.fr/en/publication/4438/download/rs-publi-4438.pdf

the action of Member States and the information made available to citizens and businesses. Furthermore, in the context of the budgeting policies of each organisation, limited resources also hamper the possibility to invest as needed in the cooperation and coordination mechanisms, leading to an overall insufficient cooperation and coordination across Member States and EU institutions.

- Insufficient education and awareness programmes. The lack of adequate education and awareness programmes, together with the lack of sufficient data and analyses, leads to the insufficient awareness of cyber threats. There is not such a culture of embedding basic measures of cybersecurity among the key learnings for the citizens of the digital society and the pace at which people become aware of cyber threats and possible remedies is much slower than the one at which they embrace technological innovations.

2.4. What are the problems for action?

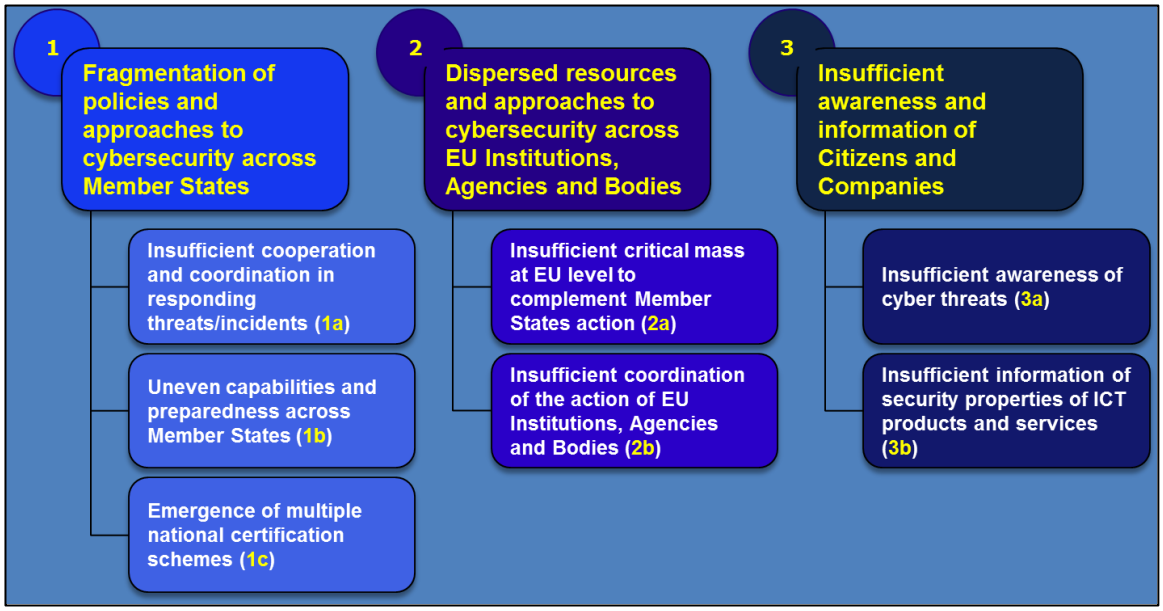
Within the broader course of action defined by the review of the EU cybersecurity strategy, and within the limits of the available instruments, the present initiative aims to **contribute to tackling** the following **interrelated problems**:

- **Fragmentation** of policies and approaches to cybersecurity across the **Member States.** This problem, highlighted by stakeholders (see Annex 2 presenting results of stakeholders' consultation), covers several aspects that are under remit of ENISA (support to cooperation among Member States, EU level capabilities to support Member States, coordination between the EU bodies, support in implementation of legislation) and specifically the policy on certification (emergence of multiple national certification schemes and initiatives that are not recognised across EU in a coherent manner).

- **Dispersed resources and approaches** to cybersecurity of the **EU institutions, agencies and bodies.**

- Insufficient **awareness** among citizens and companies of **cyber threats and insufficient information concerning the security properties of ICT products and services** they purchase.

Figure 3 Problems to tackle



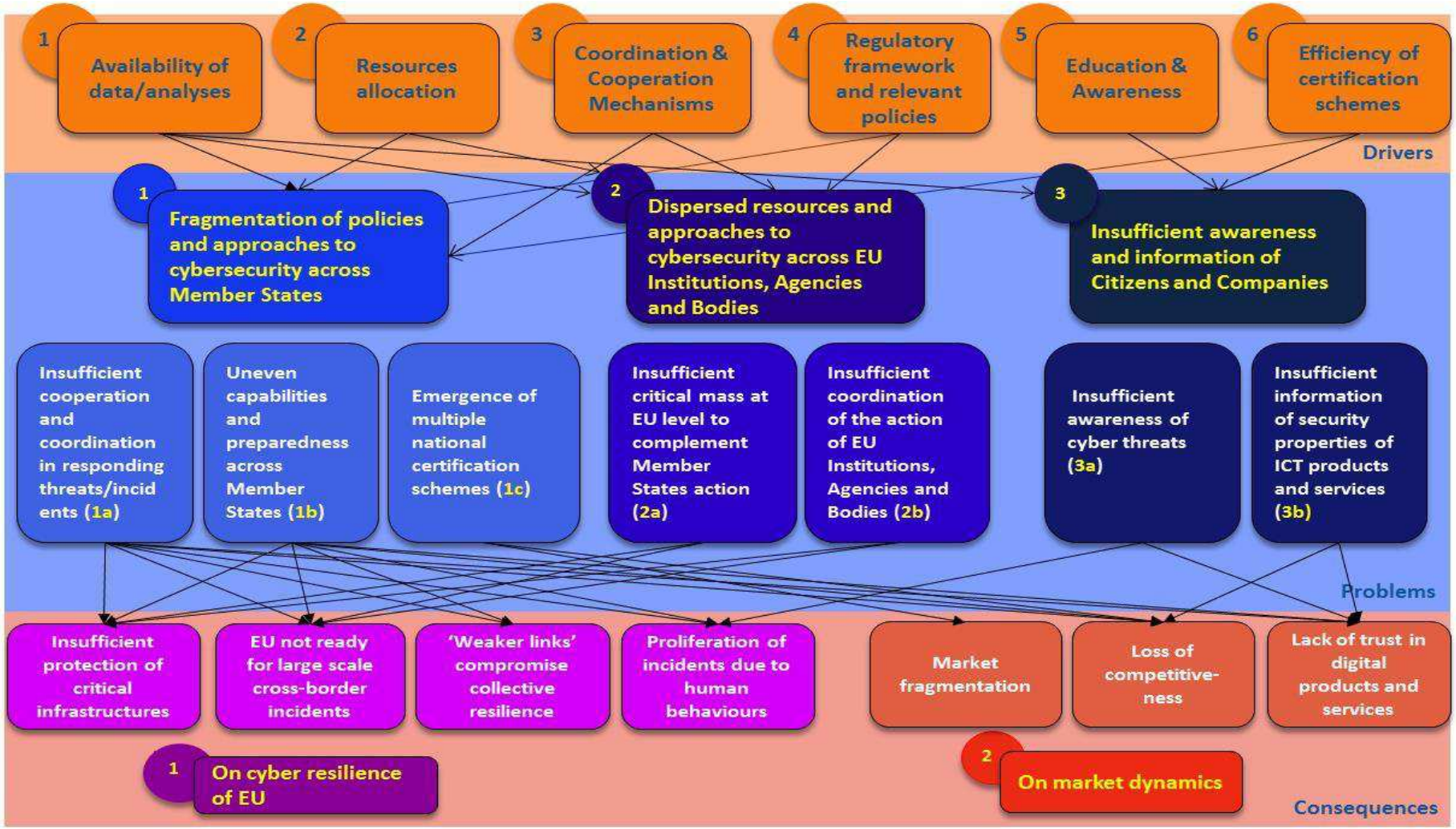
The three problems in turn lead to a series of consequences related to cyber resilience and market dynamics (see also figure 4):

- **Cyber resilience:** The fragmentation of policies and approaches at both national and EU level, together with a continuing lack of awareness of cybersecurity issues among individuals and organisations lead to the insufficient protection of critical infrastructures, the potential proliferation of incidents due to human behaviour, the exposure of the whole system to the effects of incidents due to "weaker links" in other words less equipped parts, and to a lack of preparedness of the EU to face large scale cross-border incidents.

- **Market dynamics:** The emergence of multiple national certification schemes which are not recognised throughout the EU may lead to single market fragmentation and - due to the fact that ICT vendors might need to undergo several certification processes to be able to sell in several Member States - a loss of competitiveness for the businesses, in particular for SMEs. The lack of information on security properties of ICT products and services in a context of growing cyber threats undermines the trust of users (both citizens and businesses) in digital products and services**.**

The impact of each sub-problem on the cyber resilience and the market dynamics are explained more in detail in the following sections.

Figure 4 Problem Tree



2.4.1. Problem 1: Fragmentation of policies and approaches to cybersecurity across Member States

Problem 1.a: Insufficient cooperation and coordination in responding to cyber threats and incidents.

Cybersecurity is a truly global issue, which is cross-border by nature and is becoming increasingly cross-sector due to the interdependencies between networks and information systems. The impact of incidents that affect one organisation can easily spread to others and the same logic applies to countries.

When it comes to attacks, as shown in several cases including the most recent ransomware campaign, **the perpetrators often tend to collaborate** internationally by sharing information, building their intelligence collectively and rapidly responding to possible counter-measures from the victims.

Despite some progress made in the past years, **the Commission cannot see the same level of cooperation and coordination on the side of public authorities and businesses** in the EU.

Since its establishment in 2004, ENISA has aimed to foster cooperation between Member States and the NIS stakeholders, including through the support of public-private cooperation. This included the technical work to provide an EU-wide picture of the threat landscape[52], the setting-up of expert groups and the organisation of pan-European cyber incident and crisis management exercises for public and private sectors exercises (in particular "Cyber Europe[53]").

The 2016 NIS Directive is a key step in building trust between Member States to stimulate information sharing, mutual learning and shared approaches to risk management. However, the scope of the NIS Directive is not all-encompassing (see table 2) and does not cover some of the key areas this initiative is addressing. To do this would require specific measures that complement the NIS Directive (see description of the preferred option in section 8).

Table 2 Scope of NIS Directive in relation to key areas

Areas	NIS- Directive scope
Cooperation	It created a framework for cooperation where there was none before (Cooperation Group[54] and CSIRT[55] Network[56]). Cooperation is voluntary only

[52]Since 2012, ENISA has developed the ENISA Threat Landscape (ETL), as a series of deliverables with the yearly threat landscape report being the major publication.

[53]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.

[54] The Cooperation Group is composed of representatives of all MSs, the Commission and ENISA and aims to foster strategic cooperation.

[55]CSIRT stands for Computer Security Incident Response Team. Tasks of a national CSIRTs (as per Annex I of NIS Directive) include: monitoring incidents at a national level; (ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and

	and no specific target was set for both the strategic and operational levels (level of ambition depends on work plans adopted by Member States)
Security Requirements and Reporting Obligations	For the first time, the NIS Directive introduced obligations on operators of essential services (OES) and digital service providers (DSPs) to take security measures and notify significant incidents. The security requirements placed on digital service providers (DSPs) are determined at EU level; for the operators of essential services (OES) each Member State may set its own requirements. The incident reporting obligations foresee that notifications are to be addressed to the national authorities.
Sectors	Not all sectors are covered (e.g. public administration) and for the sectors that are covered (energy, transport, water, healthcare, financial market infrastructure, banking) there is no specific mechanism to ensure consistency of policy approaches in areas with different level of cyber maturity (e.g. healthcare much less developed than finance and banking).
Large scale cross-border incidents and Crisis management	Not addressed
ICT security certification	Not addressed and there is no provision that stimulates increased security of ICT products and services (e.g. for digital devices and services or connected objects).
EU level action	No mechanism is foreseen to ensure better coordination of EU institutions, agencies and bodies and increase EU operational capabilities.

Better and more technical support at the EU level is also needed to help bridge the existing gaps, for example regarding the availability of reliable data and analyses on threats and incidents and of EU-wide good practices, in particular in critical sectors.

The lack of an adequate EU-wide technical support and the differences in the approaches to cybersecurity standards make it difficult to establish common baselines and security requirements, for instance, to reduce cost burdens on businesses which operate cross-border.

It is furthermore becoming clear that a variety of requirements for security certification are emerging at both the national and regional level. For example at a national level, although VPN[57] products are usually certified against international "collaborative"

incidents; (iii) responding to incidents; (iv) providing dynamic risk and incident analysis and situational awareness.

[56] The CSIRT Network, brings together CSIRTs from all MSs and CERT-EU (the Computer Emergency Response Team for the EU institutions, bodies and agencies) with the aim to foster operational cooperation. ENISA provides the secretariat to the CSIRT Network.

[57] Virtual Private Network

protection profiles (cPP)[58], vendors wanting to access the French market are typically requested to obtain an additional CSPN certification (see box 4). This process takes from six to nine months and it costs around EUR 80,000. Security products such as Hardware Security Module (HSMs) and/or the cryptographic modules they employ are typically certified to internationally recognized standards such FIPS. However, SOG-IS members request an additional CC certificate with a related vulnerability analysis. At a regional level, an Italian local public authority[59] had for example issued requirements in a public procurement procedure for security certification of a video surveillance system according to Common Criteria[60] (CC) at a low assurance level (EAL 1). It has been estimated that such a certification process takes 6 months and costs around EUR 20,000 (see Annex 7). In the absence of common ICT security requirements, authorities may decide both at which level such products should be tested and indeed whether such products should be tested at all, again leading to a situation of fragmentation and uncertainty within the EU.

Furthermore, existing mechanisms for cooperation on operational matters, in particular on detection and response to cybersecurity incidents are still limited and often restricted to close circles of CSIRTs. Despite good results in 'simulation mode', especially in the context of Cyber Europe exercises, and the initial work of the CSIRT Network, the EU is lacking a coordinated approach in case of cross-border incidents and it is today not prepared to handle a potential cybersecurity crisis, such as simultaneous attacks on critical information systems in several Member States.

The type of gaps and developments described above were confirmed by the results of the recent stakeholder consultations (see table 3 below and for more details Annex 2), in particular the public consultation. Here – notwithstanding the adoption of the NIS Directive – cooperation at different levels, including public-private cooperation, and the capacity to prevent and handle large scale cyber-attacks are still perceived as the most urgent gaps in the EU.

58 cPP is a Protection Profile developed by international technical communities

59 Provincia di Trento

60 The Common Criteria for Information Technology Security Evaluation (commonly known as CC) is an international standard (ISO/IEC 15408) for computer security evaluation. It is based on third party evaluation and envisages 7 Evaluation Assurance Levels (EAL). The CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that CC certificates are recognized by all the signatories of the CCRA. Within the current version of CCRA only evaluations up to EAL 2 are mutually recognized.

Table 3 Most urgent gaps and needs, as emerging from the stakeholder consultations

Most urgent gaps and needs in the cyber security field in the EU
Cooperation across Member States in matters related to cybersecurity
Capacity to prevent, detect and resolve large scale cyber-attacks
Cooperation and information sharing between different stakeholders, including public-private cooperation
Protection of critical infrastructure from cyber-attacks
Research, knowledge and evidence to support policy action

In addition, there are still gaps in the cooperation and information-sharing mechanisms both within the private sector, as well as between public and private actors. For example, the role of industrial players in collecting, analysing and disseminating information on cyber threats is essential, but the emergence of proper Information Sharing and Analysis Centres (ISACs) as a two-way information sharing resource between the private and public sector to support the protection of critical infrastructures is only a recent phenomenon in the EU. Closing the cooperation gap along these lines should be further stimulated both within sectors and across different sectors.

Problem 1.b: Uneven capabilities and preparedness across Member States

The persistence of gaps between Member States in terms of their cybersecurity capabilities and thus their preparedness in facing cybersecurity challenges is a longstanding issue that requires continuous attention. Today, considerable discrepancies can still be observed between Member States' cybersecurity policies, legal frameworks and operational capabilities[61]. As a consequence, the effectiveness of the measures taken at national level by one or a few Member States can be affected by the lower level of protection in another Member State, potentially resulting in a 'contagion' effect in case of serious disruptions affecting the 'weakest links' in the EU community.

The implementation of the NIS Directive will introduce some common requirements for the minimum capabilities in each Member State; namely a national strategy, a CSIRT and a NIS competent national authority. However, it is clear that Member States cannot count on the same level of resources, experience and risk management culture, which impacts directly on their level of preparedness[62]. For example, while most Member States have established operational entities, such as CSIRTs, the mission and the experience of those entities vary greatly. Also, only about half of the Member States are currently

[61] Global Cybersecurity Index & Cyberwellness Profiles, ABI Research and ITU, 2017. In the Global Cybersecurity Index, the countries are assessed based on five criteria: legal measures, technical measures, organisational measures, capacity building, and cooperation. The EU MSs present quite diverging scores, ranking in the global list from the 5th to the 84th position.

[62] Cybersecurity in the European Digital Single Market, High Level Group of Scientific Advisors, Scientific Opinion No. 2/2017.

conducting national cybersecurity exercises. Similarly, in the area of security certification, a clear gap of capabilities (e.g. in terms of expertise and conformity assessment bodies) can be noticed across Members States, thus maintaining an uneven level of preparedness.

Another significant gap is the different approach to collaboration between governments and the private sector, including those operating critical infrastructures. While the role of the industry is key in responding to cybersecurity challenges, only a few Member States have mature frameworks for public-private partnerships[63] in place.

In this area, the conclusions of the ex-post evaluation of ENISA present both positive and negative aspects. An overall positive assessment of the Agency emerges when it comes to meeting its objective of supporting Member States' capacity building. This is mainly due to the trainings provided and to the support in developing national strategies, but also by ENISA acting as a 'broker' of national good practices[64].

However, Member States have different needs and expectations when it comes to ENISA support especially on capacity building. While the most equipped ones rely little on the Agency, the less resourced or experienced Member States would need increased support, including for detection and response to cybersecurity incidents[65].

Problem 1.c: The emergence of multiple national and sectoral certification schemes

The rise of cybercrime and security threats has resulted in national initiatives setting high-level cybersecurity and certification requirements for ICT components including those used in traditional infrastructure. While products and services - for which a mandatory certification is not required - can still circulate in the internal market, the emergence of these national initiatives bears the risk of creating market fragmentation and erecting barriers for interoperability. In the absence of mutual recognition mechanisms among these schemes, one possible consequence would be that an ICT vendor needs to undergo several certification processes to be able to sell the same products or service in several Member States.

For example, the technical study that supports this impact assessment shows that smart meter manufacturers comply with three different certification schemes in three European countries. These are CPA in the UK, CSPN in France (see box 4 for a description of the schemes), and a specific protection profile based on CC in Germany. The overall cost of these certifications is about EUR 1 million, which in particular penalises small and medium sized enterprises (SMEs). This is an additional barrier to market entry. For example, in Germany, only one of the biggest smart-metering companies is embarking on various certification processes to enter other markets, all the other companies are only present in the German market.

As the reliance on digital devices increases, requirements for ICT security are expected to proliferate and cover a wide range of products and services. In the worst case, an ICT

63 EU cybersecurity dashboard, BSA, 2015.

64 In particular with regard to training to CSIRTs, ENISA has delivered 114 courses during 2014-2017. 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 MSs in creating their strategy.

65 For more information see the Staff Working Document on ENISA evaluation and the related study conducted by an external contractor.

product or service designed to fulfil cybersecurity requirements in one Member State would have difficulties to enter the market of other Member States where different requirements are in place.

Box 4 – Existing and emerging certification initiatives in the EU[66]

- The **Commercial Product Assurance** (CPA) developed in the UK is an example of national scheme which applies to commercial off-the-shelf products. According to CPA, a security product that is successfully assessed is awarded Foundation Grade certification, which means that the product has been proved to demonstrate good commercial security practice and is suitable for lower threat environments. CPA is open to all vendors, developers and suppliers of security products with a UK sales base. However, there is no Mutual Recognition Agreement for CPA, which means that products tested in the UK will not normally be accepted as certified products in other markets where a similar, but still different, security certification is required. Currently, 37 products have been certified under the CPA, 15 products are currently under evaluation.

- **Certification Sécuritaire de Premier Niveau** (CSPN)- an IT Security Certification Scheme established by the National Cybersecurity Agency of France (Agence nationale de la sécurité des systèmes d'information – ANSSI) in 2008. Its main purpose is to offer a faster and cheaper alternative for IT Security Certification as compared to the CC approach. Yearly, ANSSI receives around 50 submissions for certification under CSPN. The cost of each CSPN certification is in the region of 25.000 – 35.000 euro while duration of process is approximately of 3 months[67]. Similarly to the CPA, there is no MRA for CSPN, which means that products tested in the France will not normally be accepted in other markets.

- The **Dutch Baseline Security Product Assessment** (BSPA) scheme is intended to judge the suitability of IT security products for use in the "sensitive but unclassified" domain. The BSPA scheme is in pilot phase since 2015. The pilot is expected to end in 2017 and then the scheme will be operational. In the pilot phase

[66] A list of existing certification schemes and standards is available at Annex 11.

[67] Length and cost of process may vary depending on the product.

6 requests for certification were received. The average cost of a certification under BSPA is € 40.000. The overall process can take up to 2 months.

- **SOG-IS MRA**[68] is the main certification mechanism existing at European level. It includes twelve Member States[69] plus Norway and has developed a few protection profiles on digital products (such as digital signature, digital tachograph[70] and smart cards). Participants work together to i) coordinate the standardisation of CC protection profiles; ii) coordinate the development of protection profiles[71] whenever the European Commission launches a legislation that covers IT-security among others. Members can participate in the MRA as i) certificate consuming[72] and certificate producers[73]. Member States often request SOG-IS certification as a pre-condition to be admitted to national public procurement tenders.

- The German Federal Office for Information Security (BSI) is developing a baseline approach for low level assurance to improve the efficiency of CC evaluation.

- According to the support study, other emerging initiatives are being developed in Italy[74], Sweden and Norway.

The risk of a proliferation of national certification initiatives increases costs for businesses operating cross-border. It would generate a low incentive for them to embark on such a cumbersome process, with an overall detrimental effect on the quality and security of ICT used in Europe. Furthermore, such fragmentation would also impact the performance of evaluators, in that only a limited number of conformity assessment bodies would be able to certify against the requirements of different schemes.

In the preliminary results of a survey aimed at SMEs (see more details in Annex 2), 18 out of 46 respondents believe that the current existence of multiple ICT certification schemes represents a barrier to market entry because they are too costly and therefore not affordable for SMEs[75]. A recent ENISA survey on ICT security certification (see Annex 2 for the summary results) shows that 57% of respondents (19 out of 33) are aware of multiple existing ICT security certification schemes across EU Member States for the same product or service; 37% (12 out of 33) of the respondents replied 'No' to the same

[68] The Senior Officials Group – Information Systems Security (SOG-IS) agreement was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

[69] Austria, Croatia, Finland, France, Germany, Italy, Luxembourg, Netherlands, Poland, Spain, Sweden, UK

[70] The tachograph is a device that records the driving time, breaks, rest periods as well as periods of other work undertaken by a driver.

[71] A Protection Profile (PP) is a technical document that defines a standard set of security requirements for a specific type of product

[72] Members that only accept certificates issued by other certificate producer members but do not issue such certificates.

[73] Members that issue and accept SOG-IS certificates issued by other producers.

[74] A recent Italian decree (February 2017) promotes the establishment of a national centre for the evaluation and certification of ICT products used in critical infrastructure. Available at: https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html

[75] Six replied "lack of reference levels" while the rest of respondents did not know.

question, but expressed their preparedness to accept one single scheme, while 2 'do not know'. In the same survey, 90% (30 out of 33) of respondents agreed that mutual recognition of ICT security certification schemes is desirable at European level to address further fragmentation.

In written submissions related to the public consultation on cPPP, respondents emphasized that no reliable certification scheme exists at the moment at the European level. Others pointed to the fact that existing national schemes and security requirements act as barriers to market entry, complaining about the costs of compliance. Some of the industry associations state that further fragmentation of the market with numerous certification schemes should be avoided.

2.4.2. Problem 2: Dispersed resources and fragmentation of approaches to cybersecurity across EU institutions, agencies and bodies.

Problem 2.a: Insufficient critical mass at EU level to complement the action of Member States.

Despite the importance of cybersecurity on the European agenda, there is still a **lack of cybersecurity capabilities and instruments at European level** to complement the individual efforts by Member States. Overall, the EU investment[76] today - including in the development and the deployment of cybersecurity technology and solutions - is below the critical mass needed to protect our economy and institutions, in particular if compared to other key international players[77].

While many organisations at EU level have started to include a cybersecurity perspective in their policies and/or their operations (see next section), the European Commission has no operational capabilities, (the Europol's European Cybercrime Centre (EC3) is dealing specifically with cybercrime) and CERT-EU is responsible for the protection of the EU institutions, agencies and bodies. The only organisation with some preventive operational capabilities[78] and with the official mandate to contribute to the overall network and information security of the Union is ENISA.

ENISA has a broad mandate (see box 3 in section 1) but it is a rather small agency with one of the lowest budgets and number of staff compared to all EU agencies (Annex 3

[76] There is no clear picture of the investment from the MSs. The investment in cybersecurity is channelled through different programmes of the EU budget: about EUR 600 million have been invested in cybersecurity and cybercrime projects under the Horizon 2020 Framework Programme for the period 2013-2020; the European Structural and Investment (ESI) Funds foresee a contribution of up to EUR 400 million for investments in trust and cybersecurity; about EUR 30 million were invested in the period 2014-2017 for cybersecurity under the Digital Service Infrastructures (DSIs) stream within the Connecting Europe Facility (CEF); under the Instrument contributing to Stability and Peace (IcSP) cybersecurity and combatting cybercrime are a priority area since 2013 with an indicative allocation of EUR 21.5 million over the period 2014-2017.

[77] As an example, in the U.S.A., the Government invested over EUR 19 billion for cybersecurity as part of 2017 Budget (35% increase from 2016 in overall Federal resources for cybersecurity). Source: White House, Factsheet Cybersecurity National Action Plan.

[78] For example: the organisation of cyber exercises, the support to the CSIRT capacity building and the development of national cybersecurity strategies, the provision of advice to MSs (upon request) in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services.

shows the detailed figures per each agency). ENISA is also the only EU agency with a fixed-term mandate, which limits long term planning of its contribution to Member States and EU institutions. Moreover, the results of stakeholders' consultations also suggested that ENISA currently does not have sufficient resources to meet its broad mandate. Looking at the future, the mandate itself, conceived in a different political, legal, technological and threat landscape, cannot take into account more recent developments, including the tasks attributed to ENISA by the NIS Directive, and it does not sufficiently empower the Agency to respond to the forthcoming cybersecurity challenges.

In particular, the results of the evaluation of ENISA show that the agency needs to prioritize the demands of Member States and EU institutions, leaving at least partially the needs of private stakeholders and in particular industry aside. The industry on the other hand sees a potential important role for ENISA as a future link between the public and private sector. It could better support European businesses by providing high quality strategic analysis of threats, developing sector-specific expertise and ensuring harmonisation baseline requirements for cybersecurity across the EU. Industry sees ENISA focusing on future priority areas such as the Internet of Things, the move to big data and machine intelligence, certification, and envisages ENISA becoming more active in the educational field. Specifically, the large majority of stakeholders that were consulted on issues related to certification, envisage a role for ENISA in future policy developments in this area.

Looking ahead, the recently established Cooperation Group and CSIRTs Network could in the future add to the European level capacity by pooling resources, expertise and information. However, these remain subject to the limitations explained in the section above.

In particular when it comes to operational capabilities for the prevention, detection and response to cyber-incidents, there is currently no EU level capacity to guarantee the speed, accuracy, efficiency and effectiveness of response needed in a case of crisis. There is furthermore no European level system which for example covers: the early warning of threats and incidents; the ability to establish a common qualified picture in case of cross-border incidents; the capacity to handle communication with the public; and the ability to pool resources to help the victims of an attack.

Among the EU institutions, agencies and bodies, only CERT-EU has response capabilities but, as explained above, its mandate is limited to the protection of the institutions. CERT-EU also does not have 24/7 capabilities.

Problem 2.b: Insufficient coordination of the action of EU institutions, agencies and bodies.

The pervasiveness of digital technologies in all spheres of economy and society warrants the **mainstreaming of cybersecurity issues** into EU policies. The strategic importance of this objective, set out in the 2013 EU Cybersecurity Strategy, has been reaffirmed in the NIS Directive – that specified which organisation operating in specific 'critical' sectors would be subject to security and notification requirements[79] – and in the 2016

[79] Annex II of NIS Directive includes the following sectors: Energy: electricity, oil and gas. Transport: air, rail, water and road. Banking: credit institutions. Financial Market Infrastructures: trading venues, central counterparties. Health: healthcare providers. Water: drinking water supply and distribution.

Communication on Strengthening Cyber Resilience, which highlighted the need for continuous efforts to find cross-sectoral synergies and to mainstream cyber requirements in all relevant EU policies.

A number of instruments have already been put in place to mainstream cybersecurity issues at EU level covering: horizontal legislation, sectoral policy initiatives (e.g. in the energy and transport field), international relations, research & innovation, and EU agencies and bodies. As a consequence, many organisations in the EU ecosystem are involved and some are gaining competence in cybersecurity. Within the European Commission, two main Directorate Generals[80] are tasked with addressing overall cybersecurity and cybercrime; while at least eight Directorate Generals have started initiatives at sectoral level (see Annex 9 for detailed information). The European External Action Service (EEAS), which manages the EU's diplomatic relations with other countries outside the EU and conducts EU foreign & security policy, handles cyber defence as it relates to state activities and multinational or multilateral organisations (UN, NATO, OECD, etc.).

The same picture applies to EU agencies and bodies, where it is possible to identify four main actors dealing with cybersecurity, cybercrime and cyber defence (see table 4 below) and at least a further four which are gaining competences in cybersecurity in sectors like energy, transport and finance (see Annex 9).

Table 4 Mission of relevant EU agencies and bodies in the cybersecurity field

Body	Core Mission/activities
CERT of the EU institutions, agencies and bodies (CERT-EU)	To contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies ('the constituents') by helping to prevent, detect, mitigate and respond to cyber-attacks. It is also a member of the CSIRT Network.
European Union Agency for Network and Information Security (ENISA)	To contribute to a high level of network and information security within the Union. It is the EU network and information security agency and it works closely together with Members States and private sector to deliver advice and solutions in areas like policy, cooperation, capacity and community building. ENISA is the Secretariat of the CSIRT Network.
EUROPOL/European Cybercrime Centre (EC3)	To strengthen the law enforcement response to cybercrime in the EU and thus to help protect

Digital Infrastructure: internet exchange points (which enable interconnection between the internet's individual networks), domain name system service providers, top level domain name registries.

[80] Within the European Commission, DG CONNECT and DG HOME approach the challenges of cyberspace from a slightly different perspective. In particular, DG CONNECT is responsible for legislation, policy and R&I on cybersecurity (with a focus on cybersecurity resilience). DG HOME, with its focus on criminal law, works on reducing vulnerabilities, (criminal) threat alerts, awareness raising, ransomware-prevention advice etc. and deals with issues related to deterring and investigating cybercrime as well as the judicial follow-up.

	European citizens, businesses and governments from online crime. It provides operational and analytical support to Member States' investigations; it supports training and capacity-building; it represents the EU law-enforcement community in areas of common interest.
European Defence Agency (EDA)	To support the and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy. The EDA has a dedicated Project Team on Cyber defence with a variety of initiatives and reports as well as research activities in this area.

One of the results is that information and expertise are dispersed across several entities. As shown in Annex 4, there are over ten organisations that produce, collect and disseminate information and analyses, in some cases on the same topic and addressing the same public. Furthermore, the coordination mechanisms, where they exist, are not always adequate. For example, a conclusion from the evaluation of ENISA and the stakeholder consultations is that a good level of cooperation and coordination has been achieved between ENISA and EC3: There is almost no overlap between the two organisations, which seem to cooperate well. On the other side, there is still room for improvement in the coordination between ENISA and sectoral agencies, and between ENISA and CERT-EU. In particular, the evaluation highlighted that in spite of different scope of their mandate (one EU-wide, the other targeted to EU institutions) there is a risk of overlap between ENISA and CERT-EU in the areas of direct support and assistance to Member States' CSIRTs and cross-border operational cooperation.

Without increased cooperation and a more coordinated approach between the EU institutions, agencies and bodies, there is the risk of dispersing the efforts and decreasing the effectiveness and efficiency of their contribution to the EU's overall cyber resilience.

2.4.3. Problem 3. Insufficient awareness and information of citizens and companies.

Problem 3.a: Citizens' and companies are not sufficiently aware of cyber threats.

Those who want to learn and/or specialize in cybersecurity can nowadays enrol in almost 500 university courses and trainings across Europe[81].

At least 18 Member States organise national awareness campaigns, mostly targeting public sector (80%) but also SMEs and citizens; adults, children, adolescents[82]. At EU level, ENISA, together with partners in Member States and the European Commission, has been running the European Cyber Security Month (ECSM) since 2013. This is an EU advocacy campaign designed to raise awareness about cybersecurity issues throughout

[81] https://www.enisa.europa.eu/topics/cybersecurity-education/nis-in-education/universities
[82] Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.

the month of October and which promotes a sense of shared responsibility towards safe and informed behaviour on the Internet[83] among citizens.

The findings of a recent survey reveal that Member States' authorities believe that European cooperation needs to be extended towards more learning and support, and that the coordination role of ENISA and Europol should be strengthened, with more funds provided to these bodies for such activities[84].

However, despite cybersecurity gaining increasing prominence in the political agenda, companies' discourse and in the media, and in spite of Member States and EU actions, European citizens and companies still lack awareness and knowledge of cybersecurity issues. This knowledge gap ranges from basic steps to secure one's online presence to the financial and economic impact of cyber incidents. As an example of the first aspect, very recently a cyberattack on the UK Parliament has compromised dozens of email accounts belonging to parliamentarians who reportedly did not respect guidance issued by the Parliamentary Digital Service regarding password strength[85].

According to the Norton Cyber Security Insights Report[86], over six in ten (62%[87]) end-consumers said they believe connected home devices were designed with online security in mind. However, Symantec researchers identified security vulnerabilities in 50 different connected home devices ranging from smart thermostats to smart hubs that could make the devices easy targets for attacks.

[83] ENISA provided the following data with regard to the ECSM for the period 2013 – 2016: i) the number of cybersecurity activities taking place in October across Europe and the online outreach of the campaign increased at annual growth rate of 41%; featured press articles of European Cyber Security Month increased at an annual growth rate of 44% reaching 429 articles.

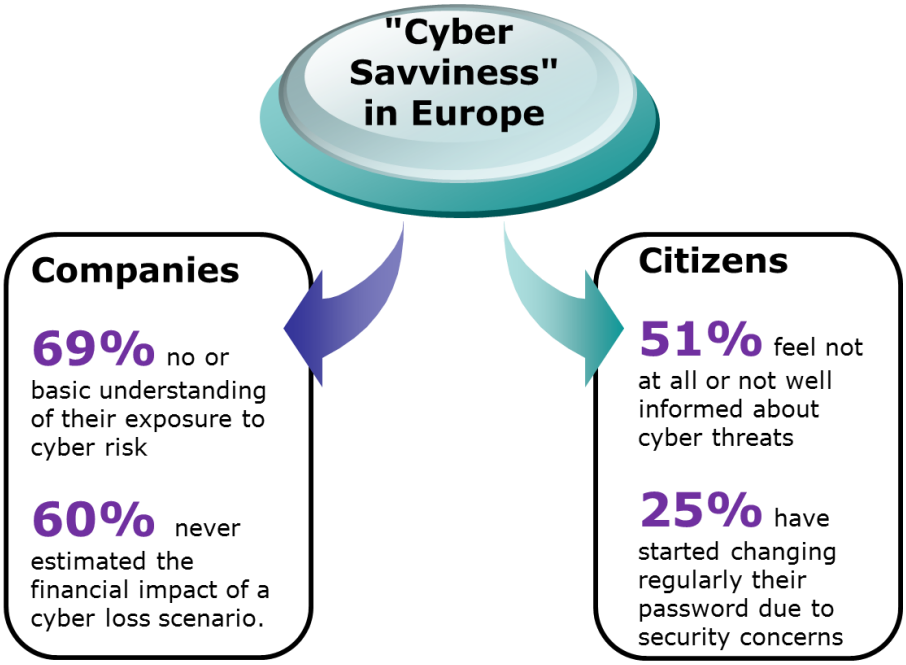
[84] Prevention and Cyber Awareness across the EU among its citizens and its SMEs, Detailed Report on the Outcome of the Questionnaire, Council of the European Union, 2017.

[85] https://www.parliament.uk/business/news/2017/june/cyber-incident/ .

[86] https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf

[87] This Report is based on an online survey of 20,907 consumers in 21 markets.

Figure 5 Some issues on awareness and knowledge of cybersecurity issues in Europe



Sources: "Special Eurobarometer 464", 2017, Attitudes towards the impact of digitisation and automation on daily life" Eurobarometer 2017, Continental European Cyber Risk Survey 2016 Report

At macro (industry) level, there is still lack of sufficient independent, neutral, EU-wide, reliable data and analyses on cyber threats, be it cross-sector or sector specific, and lack of exchange of best practices for the security of the critical infrastructures, including Internet infrastructure. Furthermore, there is a lack of systematic and reliable information on the economic impact of cyber incidents[88]. This affects investment in cybersecurity, and makes it very difficult to determine return on investments for instance from staff trainings or from equipment.

At micro (organisational) level, low security awareness of employees is considered the first factor inhibiting organizations from adequately defending themselves against cyber threats[89]. It is widely acknowledged that successful attacks are often the result of poor basic cyber "hygiene"[90]. Regular, simple security measures could significantly reduce the risks of an attack and, in the current interconnected business models, spreading the impact of a cyber-attack to other organisations. However, current cyber hygiene programmes across Europe vary and do not have a common approach[91].

The low level of awareness of cyber threats and their possible impact is a serious issue that translates in the proliferation of incidents due to human mistakes and it also contribute to the more general lack of adequate risk management practices within organisations.

[88] The cost of incidents affecting CIIs, ENISA, 2016.
[89] Cyber threat Defence Report, CyberEdge Group, 2017
[90] 'Cyber hygiene' is meant as the practice of proactively and routinely taking cybersecurity measures—to resist cyber threats and prevent online security issues.
[91] Review of Cyber Hygiene practices, ENISA, 2016.

Problem 3.b: Citizens' and companies do not have sufficient information concerning the security properties of ICT products and services they purchase (insufficient use of certification).

The security properties of an ICT product or service are difficult to assess. There is an information asymmetry between designers and vendors on one side, and customers/users of ICT solutions on the other; whereby the former has greater information than the latter regarding the security properties of an ICT product or service.

Customers lacking information cannot select their products on the basis of their real security qualities. In a targeted survey, operators of critical infrastructures[92] report that ascertaining the accuracy of the security information provided by the vendors on a specific ICT product is a major obstacle. As such, the selection of products and services tends to be based on the reputation of the vendor or on price rather than on security properties. This leads to a potential race to the bottom with regard to investments and resources allocated to security. Such a sub-optimal outcome would, in a worst case scenario, increase vulnerability. Currently, Industrial Control Systems (ICS) products - used to monitor and control electricity generation plants or transportation systems - often rely on commercial, uncertified off-the-shelf software. This results in a reduction of costs and improved ease of use, but at the same time the exposure to computer network-based attacks is increased. Such a circumstance creates a vulnerability that can be exploited to shut off power to large areas or directing cyber-attacks against power generation plants[93].

Furthermore, the co-existence of multiple schemes and standards for security certification hinders the ability of market operators and public authorities to compare and judge which ones best satisfy their particular security requirements. In April 2017, ECSO has published a State-of-the-Art Syllabus which presents an overview of certification schemes and standards in various sectors and for various products and services. For example, the document lists six schemes and two standards for security certification in the area of cloud services. Such a plethora of certification instruments translates into a missed opportunity in the digital single market. As a targeted survey shows[94], operators in the energy and finance sectors refrain from the use of cloud services due to insufficient clarity and guarantees that the available standards and schemes can satisfy certain security requirements (e.g. secure data storage).

Against this background, formal processes such as certification can contribute to increase transparency of information on the security properties of a product or a service. According to a recent ENISA survey, 81% (27 out of 33) of respondents from the certification community[95] say that, if properly designed, certification can be an effective tool to increase transparency of the level of assurance of ICT products and services and enhance trust across the digital single market (see Annex 2 for the details of the survey results). In the same survey, 66% (22 out of 33) of respondents say that greater efforts are needed to promote certification, while 21% of respondents believe that certification is a pure market issue. In the result of another survey aimed at SMEs (see Annex 2), 39 out of

[92] Preliminary results of this survey are available in Annex 7.

[93] For example, the Dragonfly attack in 2014 targeted energy grid operators, electricity generation firms, pipeline operators, across numerous countries including, Spain, France, Italy, Germany, Romania, Poland, Turkey, and United States and potentially could have led to damage or disruption to energy supplies in affected countries.

[94] Preliminary results of this survey are available in Annex 7.

[95] National certification authorities, ICT vendors, Security certification laboratory, users of ICT products and services.

46 respondents were in favour of a common label for certified ICT products[96]. According to Eurobarometer, the majority of respondents said that the security and privacy features of an ICT product play a role in their choice; 27% are ready to pay more for better security and privacy features, while 34% are not willing to pay more but these aspects have a role in their choice[97].

The suboptimal use of certification impacts the intrinsic security of the products, but also the level of information on security features of the products. To give an example, if a proper certification system had been in place throughout the EU, hospitals and other critical operators affected by the latest Wannacry attack (see section 1) would have been able to compare IT systems' security levels and, most importantly, the IT vendors' commitment to providing on-going support to users, which is not the case today.

A number of factors can explain this situation. First, existing certification schemes are to a large extent inefficient due to their high costs and lengthy processes. In addition, the current complexity of the certification landscape exacerbates such inefficiency, where separate schemes co-exist or are emerging across the EU without being mutually recognised.

These are some of the main factors which explain why ICT certification is only used in a systematic way in certain very specific domains, such as public procurement, defence and critical sectors. In many other cases, certification is left to private sector initiative, often without any involvement from public authorities and therefore without a proper monitoring on their suitability and functioning. As such, commercial/mass consumption products are rarely cyber-certified. The ever-increasing connectivity of poorly secured devices (including systems that control our cars, factories, homes, farms and critical infrastructures) could further increase the level of vulnerability of ICT devices used in Europe.

Overall, the lack of adequate information on the security properties of an ICT device can adversely affect the capacity of buyers to procure more secure products and can create a low incentive to produce more secure ICT devices. This would have a detrimental result on the level of cybersecurity of our society and economy.

2.5. Who is affected by the problem and to what extent?

Section 2.2 above presented the possible scale of cybersecurity incidents and their far-reaching impact on the economy and society. Possible failures or attacks could have an impact on a vast number of stakeholders, comprising large and small businesses, public authorities, administrations and individual citizens. In other words, everyone is concerned and potentially affected by cybersecurity issues.

Businesses

The existing gaps in the cooperation and information-sharing mechanisms within the private sector and between public and private actors limit the access to key information on cyber threats and to possible solutions for businesses to handle cyber incidents.

[96] 3 replied "no", 4 replied "don't know".
[97] Attitudes towards the impact of digitisation and automation on daily life, Eurobarometer, 2017.

They are also impacted by the dispersed resources and approaches across EU institutions, agencies and bodies since they lack adequate EU-level technical support, for example to identify threats, and to learn from EU-wide good practices. Also, businesses operating cross-border may face additional costs and different policies established at EU level if required to comply with different national security requirements.

In addition, the insufficient awareness of cyber-threats of employees and poor cyber hygiene practices within the organisations can lead to the proliferation of incidents due to human behaviour which can seriously harm the network and information security of small and large companies.

All these factors contribute to increased vulnerability of companies to cyber-threats, which, in case of significant incidents can lead to potentially huge direct financial losses, a loss of productivity, reputational damages and loss of competitiveness[98]. Beyond the costs that are currently best known – such as technical investigations, customer breaches notifications, replacement of hardware/software, legal expenses – there are less "visible" costs that can occur also once the incident has been solved: insurance premium increases, increased costs to raise debts, value of lost contract revenues, just to give a few examples[99].

Manufacturers/vendors of ICT products or providers of ICT services are affected by the emergence of multiple certification schemes since they may need to certify their products or services in several Member States. Moreover, they may find it difficult to compete for public contracts, as the tender conditions refer to specific and different security and certification requirements. In general, the fragmentation of security and certification schemes and requirements leads to additional costs for businesses operating cross-border and may thus favour local firms.

Businesses who are buyers of ICT products and services, in particular operators of essential services, are affected by inadequate certification schemes as they have little information on the security properties of the ICT devices used in their infrastructures.

Conformity assessment bodies are affected by the fragmentation of security and certification schemes as they may find it difficult to penetrate other national markets where different local security requirements and/or certification schemes are present.

Public authorities

National authorities can be impacted by the the lack of adequate European capacity to complement Member States action. This refers both to insufficient technical support, for example for the establishment of best practices or the implementation of EU policies at national level, and to the lack of hands-on support, especially for the less equipped Member States needing assistance in prevention, detection and response to cyber incidents. This situation creates inefficiencies, due to duplication of efforts (many Member States tackling issues individually) on the one side, and to limited yet dispersed resources for cybersecurity on the other.

[98] Companies do not systematically make public the costs they bear due to cyber incidents, also due to the difficulty to calculate those, but they can be very high. For example, the British telecom company Talk Talk, that had suffered an attack in October 2015, revealed to have lost 101,000 customers and suffered costs of £60m as a result of that attack. https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave

[99] Beneath the surface of a cyberattack - A deeper look at business impacts, Deloitte, 2016.

National and European public authorities can also be victims of cyber incidents and are therefore also impacted by fragmented approaches to cybersecurity and insufficient awareness of cyber threats. This can, result in direct financial losses, loss of productivity and reputational damages including critical breaches concerning national security.

Public authorities are also affected as important category of buyers of ICT products and services by the lack of sufficient information on the level of assurance of these products. Given the public interest dimension of their activities, they may wish to receive particular assurance that the solutions they procure provide a certain cyber-security assurance. They may insert in their public procurement contracts a requirement that only certified solutions are used. In case these requirements act as a barrier to foreign bidders, public bodies cannot reap the full benefits of unfettered competition and cross-border free trade across the Union.

Citizens

Citizens are still not sufficiently aware of cyber threats and how to handle them. Very often they have only a limited knowledge of basic measures, such as the need to regularly change passwords or avoiding opening attachments in suspicious emails (see section 2.2.3). According to the UK government document "Using behavioural insights to improve the public's use of cyber security best practices"[100], even people aware of security risks continue to ignore best practices (e.g. leave devices always on and online).

Citizens are therefore exposed to significant risks to bear the costs of repairing or replacing damged software or hardware, to lose and expose personal data and to direct financial losses (for example as a result of identity theft). Citizens are also affected by the lack of information on the level of assurance of ICT products and services that are on the market as they are rarely certified (see problem 3.b above). Security concerns can influence citizens' choices and prevent them to fully benefit from the advantages of digital economy and society.

EU citizens are also indirectly impacted by the multiple approaches to cybersecurity across Member States and across the EU institutions, as these can contribute to an insufficient protection of critical infrastractures and hence prevent citizens from accessing essential services (e.g. healthcare, water, energy, transport) in case of significant incidents.

[100] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf

2.6. How will the problem evolve?

The number, complexity and scale of cybersecurity incidents and their impact on economy and society are growing over time and they are expected to further increase in parallel to technological developments, for example the proliferation of the internet of things. It is predicted that cybercrime will continue rising and cost businesses globally more than $6 trillion annually by 2021[101].

This implies that the need for increased common effort from Member States, EU institutions and private stakeholders to face cybersecurity threats can only be expected to increase in the future.

With regard to the issue of cooperation across Member States, between public and private actors and across EU institutions, agencies and bodies, some progress may happen over time but at the time of drafting there is no existing plan or benchmarks in this respect. In particular, the voluntary cooperation mechanisms foreseen by the NIS Directive do not present specific targets to be achieved for both the strategic and operational levels and the level of ambition depends on work plans adopted by Member States for both the Cooperation Group and the CSIRT Network.

In absence of intervention, maintaining the status quo would imply that ENISA would remain a small agency with a broad while temporary mandate and yet key activities in the area of resilience (for example linked to policy implementation and operational cooperation) and market (in particular certification) would not be refocused according to the new context or not included at all. The Agency would therefore not be able to provide long term sustainable support to the Member States and the EU to address new threats which are horizontal in nature impacting on multiple industrial sectors.

The information asymmetry and ineffectiveness/inefficiency of the current certification schemes is unlikely to be solved in the absence of intervention. In fact, as technology becomes increasingly complex and pervasive, it will be increasingly difficult for buyers to ascertain the security qualities of ICT products and services in absence of adequate certification. Furthermore, in the absence of action, the market fragmentation is very likely to increase in the short-medium term (next 5-10 years). As technology evolves so do the cyber-threats and vulnerabilities and with them a number of national and sectorial certification schemes and requirements keep on emerging. The lack of coordination and interoperability across such initiatives on certification is an element which decreases the potential of the digital single market.

The number and scale of cyber incidents and attacks are expcted to lead to a modest natural increase in the level of awareness, due to the rising attention paid to cybersecurity issues at the level of public authorities and enterprises.

More details on the expected evolution of the problem can be found in section 5 where baseline scenarios are presented.

[101] Cybercrime Report, Cybersecurity Ventures, 2016. The estimate is based on historical cybercrime figures.

3. WHY SHOULD THE EU ACT?

3.1. Legal basis

The legal basis for EU action is Article 114 TFEU, which deals with the approximation of laws of the Member States in order to achieve the objectives of Article 26 TFEU, namely, the proper functioning of the internal market.

The internal market legal basis for ENISA has been recognised by the Court of Justice (C-217/04, judgment of 2 May 2006) and was further confirmed by the 2013 Regulation setting the current mandate of the Agency. In addition, activities that would reflect the objectives to increase cooperation and coordination and EU level capabilities to complement the action of Member States, they fall within the field of "operational cooperation". This is specifically identified by the NIS Directive (for which art 114 TFEU is the legal basis) as an objective to be pursued in the context of the CSIRT Network where "ENISA shall provide the secretariat and shall actively support the cooperation" (Article 12(1)). In particular, Article 12 (f) further identifies as tasks of the CSIRT Network: identifying further forms of operational cooperation, including in relation to: (i) categories of risks and incidents; (ii) early warnings; (iii) mutual assistance; (iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents.

The current fragmentation of the certification schemes for ICT products and services is a result of the lack of a common legally binding and effective framework process applicable to the Member States. This hinders the creation of an internal market for ICT products and services and hampers the competitiveness of the European industry in this sector.

3.2. Subsidiarity

The subsidiarity principle requires the assessment of the necessity and the added value of the EU action.

Cybersecurity is an issue of common interest of the Union. The interdependencies between networks and information systems are such that individual actors (public and private, including citizens) very often cannot face the threats, manage the risks and the possible impacts of cyber incidents in isolation. On one hand, the interdependencies across Member States, including with regard to the operation of critical infrastructures (energy, transport, water, just to name a few) make public intervention at the European level not only beneficial but needed. On the other hand, the EU intervention can bring a positive "spill over" effect due to the sharing of good practices across Member States, which can result in an enhanced cybersecurity of the Union.

In summary, in the current context and looking at the future scenarios, it appears that to **increase collective cyber-resilience** of the Union **individual actions by Member States and a fragmented approach to cybersecurity** will not be sufficient.

The respect of subsidiarity in this area was also recognised when adopting the current ENISA Regulation[102].

[102] 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.

EU action is deemed necessary also to address the fragmentation of the current certification systems. It would allow manufacturers to fully benefit from an internal market with significant savings regarding testing and redesign costs. While the current SOG-IS Agreement has achieved important results, it has also shown important limitations to be a long term suitable and sustainable solution.

The added value of acting at EU level, in particular to enhance cooperation between Member States but also between NIS communities, has been recognised by the 2016 Council Conclusions[103] and it also clearly emerges from the evaluation of ENISA.

None of the options analysed in this Impact Assessment go beyond what is necessary to achieve the objectives set in the following section in a satisfactory manner. Furthermore, the scope of EU intervention would not impede any further national actions in the field of national security matters.

EU action is therefore justified on grounds of subsidiarity and proportionality.

4. OBJECTIVES: WHAT SHOULD BE ACHIEVED?

Based on the problems identified in section 1, the following policy objectives for the current initiative have been set:

4.1. General objectives

The main policy objectives of this initiative are to:

1. **Increase the cyber resilience** of the Member States, businesses and the EU as a whole.
2. Ensure the **proper functioning of the EU internal market** for ICT products and services.
3. **Increase the global competitiveness** of the EU companies operating in the ICT field.

4.2. Specific objectives

With the general objectives in mind, in the broader context of the new Cybersecurity Strategy the initiative intends to achieve the following specific objectives:

1. Increasing **capabilities and preparedness** of Member States and businesses
2. Improving **cooperation and coordination** across Member States and EU, institutions, agencies and bodies.
3. Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.
4. Increasing **awareness** of citizens and businesses on cybersecurity issues.

[103] Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry - 15 November 2016.

5. Increasing the overall **transparency of cybersecurity assurance**[104] of ICT products and services to strengthen trust in the digital single market and in digital innovation.

6. Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.

5. WHAT ARE THE AVAILABLE POLICY OPTIONS?

5.1. What is the baseline from which options are assessed?

The instruments currently available to support Member States capabilities, cooperation and the EU cyber resilience, including those of the current ENISA Regulation and the NIS Directive, are insufficient for the current cybersecurity challenges. As presented earlier in the problem statetemet, although the NIS Directive entered into force only in July 2016, and consequently it is too early to give conclusive assessment of its effectivenenss, it does not cover all sectors and it does not necessarily include sufficient mechanisms to stimulate fully fledged EU-wide cooperation for the future cyber challenges. Also, the NIS Directive does not address the topic of ICT security certification and it does not include provisions for handling of large scale cross border incidents.

With the (upcoming) adoption of the 2017 Septemper Communication, new instruments would be in place, in particular in the field of cybersecurity resilience and response (see paragraph 1 of the report). For the purpose of this analysis, the baseline scenario would be affected by the adoption of the Recommendation on the EU cybersecurity blueprint and the (forthcoming) legal instruments to implement the European Cybersecurity Research and Competence Centre and possibly also on the Emergency Fund.

With regard to the blueprint, it is assumed that the EU will have in place a framework for coordinated response to possible large scale cross-border cyber incidents. However, the role of ENISA envisaged in the blueprint – from supporting situational awareness to handling communications – goes beyond the current mandate of the Agency. Therefore, the blueprint could not be implemented effectively without a revised mandate of the Agency or a replacement of the Agency with other similar body to perfom those functions. In the context of EU response to cybersecurity crisis situations, the baseline scenario would include – upon its adoption in the context of the next Multiannual Financial Frameword - the Cybersecurity Emergency Fund that would allow Member States to seek help at the EU level in case of major incident, provided that the Member State had put in place a prudent system of cybersecurity prior to the incident, including full implementation of the NIS Directive, mature risk management and respective supervisory frameworks at national level. The Fund could deploy a rapid response capability in the interests of solidarity and finance specific emergency response actions such as replacing compromised equipment or deploying mitigation or response tools to assist victims.

[104] Transparency of cybersecurity assurance means providing users with sufficient information on cybersecurity properties which enables users to objectively determine the level of security of a given ICT product, service or process.

In the field of research and development, upon the adoption of the related legal instrument, ENISA (both in case of existing and revised mandate) would links its efforts in the area – maninly advisories on EU needs – to the work the European Cybersecurity Research and Competence Centre, which would become a major player by pooling and shaping research efforts and supporting the development of industrial capabilities.

Article 36 of the current ENISA Regulation includes a sunset clause, fixing the duration of the agency mandate for seven years until June 2020. For the purpose of this analysis, the status quo, which sees the existence of an EU decentralised agency with a fixed term mandate, is considered as baseline scenario. The sunset clause and thus termination of ENISA is also explored among the possible options.

With specific regard to certification, the baseline scenario translates into non-EU action. In this case, it is unlikely that ICT producers would establish self-regulatory measures to allow buyers to better ascertain the security qualities of ICT products and services. It is however possible that Member States take action, which could result in even more national and sectoral only certification schemes. In this case, fragmentation is expected to widen in the short-medium term (5-10 years) with a negative impact on the full potential of the digital single market.

The current SOG-IS agreement and the CCRAs are also unlikely to constitute a possible solution to the problem in the short and medium term. As explained above, the SOG-IS MRA is based on the methodology of CC, thus it shares similar criticism related to the length of process, high cost, unsuitable for products requiring low level of assurance, suitable to certify products rather than services. For these reasons, only a few protection profiles related to digital products have been developed under the current SOG-IS MRA. These are for example, digital tachographs, digital signatures and smart cards.

5.2. Policy options related to ENISA

The policy options on the possible future of ENISA, including those that were discarded as result of the impact assessment exercise, are presented below.

Option 0 – Baseline scenario

This option is about the preservation of the status quo. ENISA would continue to be an Agency with a mandate limited in time. ENISA's mandate would be extended in a manner similar to the previous renewals (Regulation (EC) No 1007/2008 and Regulation 580/2011) and the objectives and tasks of the Agency would be largely similar to the ones of today subject to adaptations based on acts that entered into force after the adoption of the current ENISA Regulation in particular the NIS Directive and the Regulation on electronic identification and trust services for electronic transactions in the internal market[105] (eIDAS Regulation). It might also include provisions from the Electronic Communications Code, which is currently in the legislative process and therefore not yet adopted. Preserving the status quo would also imply maintaining a fixed-term mandate for ENISA. Therefore, the activities described in the box below would also be subject to a time limit.

[105] Regulation EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

1. ENISA's mandate, currently expiring in 2020, would be extended for a fixed term period based on previous mandates.

2. The current mandate, objectives, governance and organisation of the Agency would remain unchanged.

3. The tasks of the Agency would remain mostly unchanged, except for additional tasks due to alignment with the specific provisions of relevant laws:

- As provided by the NIS Directive, ENISA would support Member States at their request, in developing national strategies or national CSIRTs.

- As provided by the NIS Directive, ENISA would provide the secretariat of the CSIRTs network and actively support the cooperation among national CSIRTs. ENISA will also be part of the Cooperation Group, with a view of supporting strategic cooperation between national competent authorities.

- As provided by the Framework Directive for Electronic Communications (the new Electronic Communication Code is currently in the legislative process), ENISA would be required to contribute to an enhanced level of security of electronic communications by providing expertise and advice, and promoting the exchange of best practices.

- As provided by the eIDAS Regulation, ENISA would collect summary information from supervisory bodies on the notifications of security breaches.

Option 1 – No policy intervention –Expiry of ENISA's current mandate without renewal and termination of ENISA

This option would not entail a new legislative proposal to amend or repeal the current ENISA Regulation. This would lead to the termination of ENISA at the end of its mandate in June 2020 (seven years from 19 June, 2013 in accordance with article 36 of ENISA Regulation). The Commission would then need to decide on the possible redistribution of competences/activities at EU and/or national level. To be noted that according to the provisions of the Common Approach on decentralised agencies "closing down an agency could be a solution for dealing with underperforming agencies unless the agency is still the most relevant policy option, in which case the Agency should be reformed"[106]. In this case and in the absence of a new proposal, in accordance with the current Regulation (recital 54 to be in footnote) the Commission should take the relevant measures addressing in particular issues relating to staff contracts and budget arrangements.

1. If a decision is taken not to extend ENISA's mandate, pursuant to art. 36 of the ENISA

[106] Joint Statement of the European Parliament, the Council of the European Union and the European Commission on decentralised agencies – Common Approach – 2012.

Regulation, it would expire as of 19 June, 2020.

2. As provided by the 'sunset clause'[107] of the ENISA Regulation, the Agency and the Commission should take the relevant measures towards the end of the current mandate, addressing in particular issues relating to staff contracts and budget arrangements.

3. The tasks currently attributed to ENISA would be terminated and, in the absence of EU intervention, fall back under the responsibility of Member States.

4. The tasks attributed to ENISA by subsequent legislation, in particular by the NIS Directive, would have to be re-assigned to other EU or national bodies. This would entail the repeal of the Regulation and a new proposal for NIS Directive with a new arrangement for what concerns ENISA. Such a proposal would need to be prepared in time for there not to be a gap affecting the proper implementation of NIS Directive due to take place in May 2018.

Option 2 – 'Reformed ENISA'

This option would reform the Agency building on the strengths emerged in the course of the current mandate and addressing shortcomings and weaknesses. The new mandate would take into account new threats, policy, actors and technology changes as well as the results of the evaluation.

In particular, this would imply a redefinition of ENISA's role, competences and functioning, scope, the duration of the mandate, as well as the synergies with other EU agencies and bodies.

1. ENISA would be granted a permanent mandate and thus be put on a stable footing for the future. The mandate, objectives and tasks would still be subject to regular reviews.

2. The mandate would further clarify the role of ENISA as the EU agency for cybersecurity and as the reference point in the EU cybersecurity ecosystem, acting in close cooperation with all the other relevant bodies of such ecosystem.

3. The organisation and the governance of the Agency, which were overall positively judged in the course of the evaluation, would be moderately reviewed, in particular to make sure that the needs of the wider stakeholders' community are better reflected in the work of the Agency. This would imply, for example, the need that the Executive Director and the Management Board take into utmost account the opinion of the Permanent Stakeholder Group (PSG) in the preparation of the annual and multiannual work programme, as well as enabling the participation of a limited number of PSG members as observers in the Management Board, upon request of the Chair.

4. The scope of the mandate would be delineated, strengthening those areas where the agency has shown clear added value and adding those new areas where support is needed in view of the new policy priorities and instruments, in particular the NIS Directive, the review of the EU Cybersecurity Strategy, the upcoming EU Cybersecurity Blueprint for cyber crisis cooperation and ICT security certification:

[107] According to the Common Approach on decentralised agencies, founding acts should include review or sunset clauses. The sunset clause refers to the possible termination of the activities of an agency at the end of the mandate, as established in its founding act.

- EU policy development and implementation: ENISA would be tasked with proactively contributing to the development of policy in the area of Network Information Security, as well as to other policy initiatives with cybersecurity elements in different sectors (e.g. Energy, Transport, Finance, etc.). To this end, it would have a strong advisory role, including the provision of independent opinion and preparatory work for the development and update of policy and law. ENISA would also support the EU policy and law in the areas of electronic communications, electronic identity and trust services, with a view of promoting an enhanced level of cybersecurity. In the implementation phase, in particular in the context of the Cooperation Group, ENISA would assist Member States in achieving a consistent approach to the NIS Directive implementation across borders and sectors as well as other policy and laws where cybersecurity is involved. In order to support the regular review of policy and law in the area of cybersecurity, ENISA would also provide regular reporting on the state of implementation of the EU legal framework.

- Capacity building: ENISA would be contributing to the improvement of EU and national public authorities' capabilities and expertise, including on incident response and supervision of cybersecurity related regulatory measures. The agency would also be required to contribute to the establishment of Information Sharing and Analysis Centres (ISACS) in various sectors by providing best practices and guidance on available tools, procedures as well as appropriately addressing regulatory issues related to information sharing.

- Knowledge and information, awareness raising: ENISA would have a new task in developing the information hub of the EU. This would imply the promotion and sharing of best practices and initiatives across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies; the Agency would also make available advice, guidance and best practices on the security of critical infrastructures. In the aftermath of significant cross-border cybersecurity incidents, ENISA would also compile reports with a view of providing guidance to businesses and citizens across the EU. This stream of work would involve also the regular organisation of awareness raising activities in coordination with Member States authorities.

- Market related tasks: ENISA would perform a number of functions specifically supporting the internal market, which would include new tasks: cybersecurity 'market observatory', by analysing relevant trends in the cybersecurity market to better match demand and supply; support the EU policy development in the ICT standardisation and ICT security certification areas. In particular, it would facilitate the establishment and uptake of security standards. ENISA would also execute the tasks foreseen in the context of the future framework for certification (see below section 5.3 – options for certification).

- Research and innovation: ENISA would contribute its expertise by advising EU and national authorities on priority-setting in research and development, including in the context of the contractual public-private partnership on cybersecurity. ENISA's advices on research would feed into the new European Hub of Excellence in Cybersecurity, as developed in the context of the review of the Cybersecurity Strategy, ENISA would also be involved, when asked to do so by the Commission, in the implementation of research and innovation EU funding programmes.

- Operational cooperation and crisis management: this stream of work would build on the existing preventive operational capabilities, in particular the pan-European

cybersecurity exercises (Cyber Europe), and a supporting role in operational cooperation as secretariat of the CSIRTs Network (as per NIS Directive provisions) by ensuring, among the others, the well-functioning on the CSIRTs Network IT infrastructure and communication channels. In this context, a structured cooperation with CERT-EU, EC3 and other relevant EU bodies would be required.

Furthermore, a structured cooperation with CERT-EU should result in a function to provide technical assistance in case of significant incidents and to support incident analysis. Member States that would request it would receive assistance to handle incidents and backend support for analysis of vulnerabilities, artefacts and incidents in order to strengthen their own preventive and response capability. In cooperation with the CSIRT Network, ENISA would also conduct ex-post technical enquiries of significant incidents with a view to issue recommendations in order to prevent future incidents.

ENISA would also play a role in the upcoming EU cybersecurity blueprint, setting the Commission's proposal to Member States for a coordinated response to large-scale cross-border cybersecurity incidents and crises at the EU level[108]. . ENISA would facilitate the cooperation between individual Member States, in dealing with emergency response by analysing and aggregating national situational reports based on information made available to the Agency on a voluntary basis by Member States and other entities.

Option 3 – EU cybersecurity agency with full operational capabilities.
This option implies restructuring ENISA according to the model that several Member States have adopted, by bringing together three main functions: 1. policy advisory 2. the centre of information and expertise and 3. the Computer Emergency Response Team. In this case, the Agency would cover the entire cybersecurity lifecycle and deal with prevention, detection and response to cyber incidents.

1. The new ENISA would be granted a permanent mandate. The mandate, objectives and tasks would be subject to regular reviews.

2. The organisation and the operations of the Agency would be reviewed, in particular to ensure that the needs of the wider stakeholders' community are better reflected in the work of the Agency.

3. To a large extent this option would imply the same change in the scope of the mandate as option 2 (policy support, capacity building, market, knowledge and awareness raising) however additional tasks would be added in the area of incident response and crisis management.

4. The new operational tasks of ENISA might require a new legal basis for the corresponding Regulation.

[108] The "blueprint" will apply to cybersecurity incidents whose disruption is more extensive than any Member State can handle on its own or affects two or more Member States with such a wide-ranging and significant impact or political significance that they require timely policy coordination and response at Union political level.

5. The new ENISA would be in a position to provide fully-fledged CERT services, adapted to its EU-level mission ensuring no duplication with the tasks of national CERTs, such as:

    - Establish and provide its own sources of information related to cybersecurity incidents and threats.

    - Produce real-time situational awareness and dynamic (live) threat intelligence feeds (accessible to national CSIRTs and possibly CSIRTs of private entities like the operators of essential services) based on ENISA's own sources as well as information that is mandatorily shared with the Agency during large scale cybersecurity incidents and crises.

    - Provide active technical operational assistance, both in terms of technical expertise as well as human resources to Member States CSIRTs (and possibly to other actors like operators of essential services, EU bodies and institutions), in preventing, detecting and particularly in responding to incidents.

    - Coordinate CSIRTs Network operations, pooling national resources on analysing threats and responding to incidents.

5.3. Options related to certification

The results of the consultations with national certification authorities, ICT vendors and providers, operators of critical infrastructures (see Annex 2) as well as inputs of technical support studies and reports (e.g. by JRC and ENISA) have been used to select the most appropriate policy options to address the problems identified in this Impact Assessment. These options respond to the need to promote security certification through agile and flexible mechanisms on the one hand, as well as the desire to support an EU-wide approach to security certification that builds as much as possible on existing mechanisms, on the other hand.

On this basis, the following policy options were considered to achieve the policy objectives and to address the problems identified.

<u>Option 0</u>: Baseline scenario - Do-nothing.

Under this option the Commission would not undertake any policy or legislative action. With regard to the three identified problems, this option would result in the following situation:

1. The problem of **market fragmentation is very likely to increase** in the short-medium term (next 5-10 years), as a number of national and sectoral certification schemes and competing sectoral standards are emerging[109].

2. The co-existence of competing schemes and standards would undermine the ability of vendors and end-users (citizens and operators of critical infrastructures) to compare and

[109] For a full overview of existing cybersecurity sectoral standards and certification schemes see here: www.upm.es/observatorio/vi/gestor_general/recuperar_archivo.jsp?idf=642&tipo=2

judge which scheme or standard would best satisfy their particular security requirements This circumstance would worsen the problem related to information asymmetry.

3. The lack of coordination would cause a situation where Member States continue to put in place certification requirements for their critical infrastructures through public procuremeents, thus creating an uneven level of protection. As Member States are increasingly interconnected, this scenario would increase vulnerability and the risk of a cross-border proliferation of attacks (esp. on critical infrastructures), even in those Member States adopting high level of security requirements.

4. The lack of coordination and interoperability across multiple schemes and standards would not contribute to create a chain of trust in the digital single market. A divide may persist between operators of critical infrastructures - which increasingly rely on digital products and services for their operations - and vendors or providers. This may hamper the digital single market

5. Agreements establishing mutual acceptance of certificates among Member States should be expected in the future. However, they will occur in an uncoordinated manner and would depend on the willingness of each Member States. For example, the German national baseline certification scheme (under development) is likely to be mutually recognized with the existing French national scheme (CSPN), but not necessarily with similar British scheme (e.g. Baseline Security, CPA). Such a piecemeal approach may turn out to be inefficient and resource-intensive

6. Market operators will put in place self-regulatory measures or embark on certification processes only in presence of strong economic incentives such as compliance with public procurements requirements which would limit the roll-out and possible positive impact of ICT certification.

7. The effectivenss and efficiency of current certification mechanisms such as SOG-IS MRA and the CCRAs will not improve in the short and medium term. The shortcomings of CC - on which SOG-IS MRA is based - related to high cost, long duration of process, limited membership and scope will remain.

Option 1: Non-legislative ("soft law") measures. Under this option, the Commission would use soft policy instruments to reach the objectives of this initiative (e.g. improve the level of information related to the security pproperties of ICT devices and reduce fragmentation). As such, the Commission could issue interpretative guidelines, encourage co- or self-regulation initiatives, promote the development of technical standards, support reasearch or awareness rising activities. The specific contents of the individual measures cannot be delineated with precision at this stage, as they will emerge as a result of the overall process within the Commission and with the stakeholders.

1. **Issuing interpretative communications**: The Commission would provide guidance on elements of national or sectorial schemes, such as in particular requirements for certification authorities and conformity assessment bodies. The Commission would request ENISA to provide a preliminary assessment of such interpretative communications and to explore the views of public and private stakeholders by means of workshops and formal consulations.

2. **Support EU-wide co- or self-regulatory initiatives:** together with ENISA, the Commission will support, and incentivise the establishiment of voluntary EU-wide schemes for the certification of ICT products and services so as to foster the emergence of EU-wide solutions. The Commission may also initiate co-regulatory activities, thus entrusting the development of a specific certification scheme to economic operators. However, under such scenario, the system in place would include a dedicated supervisory mechanism.

3. **Strengthen standardisation activity:** the Commission would further intensify and support the adoption of EU standards in the field of security of ICT products and services with a view to harmonising the substantive requirements at EU level. The Commission could define the need of EU standards on the basis of the recommendations from the Focus Group on Cybersecurity established by CEN/CENELEC/ETSI[110], for example. The Group's recommendation will also take into account inputs from ENISA.
4. In order to **avoid duplication and ensure coherence**, the above activities should be carried out in close consultation with institutional actors responsible for certification initiatives stemming from other legislation (e.g. GDPR) and from other sectoral legislation on security of critical infrastructures[111].
5. **Research and awareness-raising activities**. The Commission would increase the funds related to R&D projects in the field of ICT security certification. In addition, ENISA would be tasked with carrying out awareness-raising activities such as setting-up an ad hoc website, online advertising campaign, ad hoc conferences, events and training for national officials.

Option 2: EU legislative act to create a mandatory system for all Member States based on the SOG-IS system.

Under this policy option, the Commission would propose a legislative act that would incorporate SOG-IS MRA so that it becomes binding on all Member States. Therefore, the Management Committee of the current SOG-IS MRA will be composed of representatives from all Member States. Sectoral Working Groups will provide technical support to the Management Committee. ENISA would help run the Secretariat of the Management Committee and would support the coordination of activities of the Working Groups.

The legislative act will have the following essential content:

1. Lay down rules of **participation**: representatives from Member States can participate in two fundamental ways: as certificate consuming participants and as certificate producers
2. Lay down the requirements that Member States have to comply with when designating **certification authorities** and **testing facilities**;
3. Refer to **CC** as the applicable security evaluation criteria.
4. Establish the objectives and roles of the Management Committee such as:
    a. Coordinate the standardisation of CC protection profiles
    b. Coordinate the certification policies between national Certification Bodies
    c. Coordinate the development of protection profiles whenever the European Commission launches a directive that should be implemented in national laws and that includes aspects related to information security
    d. Define role of the Management Committee in international fora such as CCRA
5. Establish **general rules for mutual recognition** of certificates issued under the new SOG-IS system;
6. Lay down provisions to initiate consultations with other institutional actors to seek

[110] https://www.cencenelec.eu/standards/sectors/defencesecurityprivacy/security/pages/cybersecurity.aspx
[111] For example, consultations may be conducted with the future European Data Protection Board or other authorities in charge of security of critical infrastructures.

coherence with other certification initiatives deriving from other legislation.

Option 3: EU general ICT cybersecurity certification framework

Under this option, the Commission would propose a new European ICT Security Certification Framework laying down rules for the development of individuals EU-wide cybersecurity certification schemes for specific ICT products and services or cybersecurity risks, leading to the issuance of certificates valid and recognised in the whole EU.

A European Cybersecurity Certification Framework (the "**Framework**") for ICT products and services and specifies the essential functions and tasks of ENISA in the field of cybersecurity certification. The Framework lays down common provisions and procedures enabling the creation of EU-wide cybersecurity certification schemes for specific ICT products/services or cybersecurity risks. The creation of European cybersecurity certification schemes in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.

A European cybersecurity certification scheme shall be understood as the comprehensive set of rules, technical requirements, standards and procedures defined at Union level applying to the certification of ICT products and services falling under the scope of the scheme. As such, the type of ICT product and service covered by a European certification scheme will be defined in the approved scheme itself. Moreover, it is essential to underline that certification schemes do not, as a rule, set the technical standards, i.e. they do not lay down the technical requirements that the products need to comply with. This is the task of legislation and technical standardisation.[112] Certification schemes set out, insetad, a specific process for evaluating – at a specific level of assurance - the security properties of ICT products and services falling within the scope of the scheme[113] Evaluation of security functionalities of these products or services would be carried out against the requirements to which a particular scheme will refer. Existing standard can be used when considered appropriate to express these technical requirements ..

The main elements of this option are specified in more detail below:

1. The proposal does not introduce directly operational certification schemes, but rather creates a system (framework) for the establishment of specific certification schemes for specific ICT products/services (i.e. "European cybersecurity certification scheme"). The creation of individual European cybersecurity certification schemes in accordance with the Framework will allow certificates issued under those schemes to be valid and recognised across all Member States and to address the current market fragmentation.
2. The framework would apply in so far as there are no specific provisions with the same

[112] In the case of European standards, this agreement is reached within the so-called European standardisation organisations and endorsed by the European Commission by means of its publication in the Official Journal (see Regulation 1025/2012).

[113] i.e. for testing the security functionalities of ICT products and therefore to establish the required level of confidence

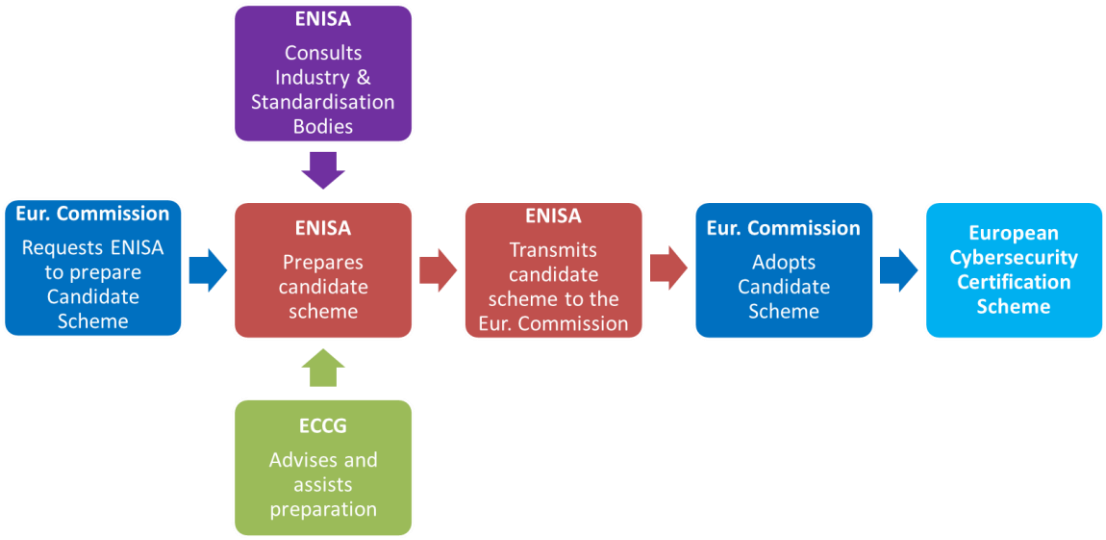
objective in Union legislation. The priorities of the certification framework will be identified by Member States, the Commission or ENISA on the basis of the perceived needs of Member States or emerging from the market. The initial ideas on the priority areas for certification which derive from public consultations as well as discussions with Member States and the industry are presented in the 2017 September Communication that is adopted as part of the cybersecurity package[114].

3. The general purpose of a European scheme would be to attest that the ICT products and services that have been certified in accordance with such schemes comply with specified requirements (as detailed for instance in an European standard) as regards their ability to resist at a given level of assurance, and actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via those products, processes, services and systems.

4. The proposal will lay down a specific set of security objectives, which should be taken into account in the design of a specific European scheme. They will include, for instance, the ability to protect data stored, transmitted or otherwise processed against accidental or unauthorised storage, processing, access, disclosure, destruction, accidental loss or alteration.

5. The proposal will also provide the minimum content of European schemes. In particular, such schemes will have to include a number of specific elements setting out the scope and object of the certification, including the categories of products and services covered the specific evaluation criteria and evaluation methods, the level of assurance basic, substantial or high intended to ensure as well as a detailed description of technical security requirements, for example by reference to standards or technical specifications.

6. European schemes would be prepared by ENISA, with the assistance and close cooperation of the European Cybersecurity Certification Group (see below), and adopted by the Commission by means of delegated or implementing acts. In practice, the Commission may request ENISA to prepare a scheme for specific ICT products/services or cybersecurity risks. ENISA will work on the scheme closely in cooperation with national certification bodies represented in the European Cybersecurity Certification Group. Member States and the Group may also propose to the Commission that it requests ENISA to prepare a particular scheme.



[114] JOIN(2017) 450

Figure 6 Overview of a how a European cybersecurity certification scheme is adopted

7. Recourse to European cybersecurity certification would remain voluntary. However, future Union or national legislation may mandate the use of an approved European scheme for specific products or services. As such, no specific measures are foreseen nor are necessary for relevant products not covered by an EU certification scheme. However, in order to ensure harmonisation and avoid fragmentation, Member States should not introduce new national certification schemes for ICT products and services where an European cybersecurity certification scheme for the same product or service exists. Similarly, current national schemes or procedures for the ICT security certification of products and services will cease to produce effects where a European cybersecurity certification scheme for the same product or service will be established. Existing certificates issued under current national cybersecurity certification schemes shall remain valid until their expiry date. The creation of national schemes with high level of assurance remains possible if introduced on the ground of national security.
8. Once a cybersecurity certification scheme is adopted, manufacturers of ICT products or providers of ICT services will be able to submit an application for certification of their products or services to a conformity assessment body of their choice. Conformity assessment bodies should be accredited by an accreditation body in accordance with Regulation 675/2008/EC. Accreditation bodies should revoke an accreditation of a conformity assessment body where the conditions for the accreditation are not, or are no longer, met or where actions taken by a conformity assessment body infringe this Regulation.
9. Under this option, Member States would have to provide for one certification supervisory authority, tasked with supervising compliance of conformity assessment bodies and of the certificates issued by conformity assessment bodies established in their territory, with the requirements of this Regulation and of the relevant European certification schemes. National certification supervisory authorities should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories. Moreover, they should cooperate with other certification supervisory authorities or other public authorities by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.
10. **European Cyber-certification Group** (ECCG): the proposal establishes the European Cyber-certification Group (ECCG), consisting of representatives of certification authorities of all Member States. The main task of the Group would be to advise the Commission on issues concerning cybersecurity certification policy and to work with ENISA on the development of candidate European cybersecurity certification schemes. ENISA would assist the Commission in providing the secretariat of the Group and would maintain the inventory of schemes approved under the Framework. ENISA would also liaise with standardisation bodies to ensure the appropriateness of standards used in approved schemes and to identify areas in need of certification schemes and cybersecurity standards.

Option 4: ICT security internal market legislation

Under this option the Commission would propose an EU ICT security legislation based on the 2008 internal market New Legislation Framework. As a result of this option, selected ICT products and services could only be put on the market if they comply with identified essential requirements on the basis of a prior conformity assessment. This would entail adding a new requirement for compliance with an ICT security standards to the other requirements needed to obtain the CE mark. In line with the approach of the

new legislative framework, the law would rely on standards[115] and would establish a presumption that compliance with such standards implies compliance with the EU internal market. The main elements of such legislation are discussed below:

1. **Essential requirements** for the **construction and provision** of ICT products and services. Such requirements would concern mainly security, privacy, transparency and safety.
2. Requirements relating to the **provision of information to Member States**, the Commission and consumers.
3. Requirements concerning the **registration** and **traceability** of ICT products and services.
4. Requirements that ICT products and services cannot be placed on the market if they do not comply with the requirements of the legal instrument.
5. **Specific obligations of manufacturers, importers and distributors** with regard in particular to the declaration of conformity and the affixing of the CE mark.
6. Provisions concerning **market surveillance**, including the appointment by MS of supervisory bodies, conformity assessment bodies, measures for correcting, withdrawing or recalling non compliant products and services.

5.4. Options discarded at an early stage

In the course of the impact assessment exercise two of the policy options identified in the previous section were discarded at an early stage and thus were not subject to deeper analysis and assessment.

- **Option 1 '<u>Expiry of ENISA mandate</u>'**. This option has been discarded for several reasons. First of all from the evaluation it emerged that the Agency showed to be relevant and to provide EU added value and that, if its weaknesses are addressed, ENISA has the strong potential to contribute even more to increase cybersecurity in the EU. The need for even further cooperation, including at operational level, is one of the key findings of the evaluation. This concluded that it would not be possible to ensure the same degree of community building and cooperation across the Member States without a more centralised EU agency for cybersecurity; the picture would be more fragmented with bilateral or regional cooperation stepping in to fill a void left by ENISA. ENISA is in fact the only EU agency that currently can ensure EU coordination and the needed cross-border approach.

  Secondly, the option of terminating ENISA would be incoherent with the provisions of the NIS Directive, which require ENISA to perform tasks that have no end date. Some of the tasks conferred upon ENISA by the NIS Directive could be performed by the Commission. However, this would be incoherent with the decision of the co-legislators that specifically assigned those to an independent EU agency. The termination of ENISA - and in the that case it would not be replaced by an equivalent EU level body - would also imply less EU level support

[115] This option would also encourage the development of standards, in case they do not exist for specific products

in the field of cybersecurity and, as such, be in contrast with the vision expressed in the review of the EU Cybersecurity Strategy. In particular, it would be incoherent with the EU cybersecurity blueprint for large scale cross-border incidents, which foresees a role for ENISA in supportive a cooperative Union response to such incidents.

Thirdly, with regard to the EU budget, the discontinuation of ENISA would imply the disinvestment of the current contribution to ENISA budget (about EUR 11 million per year). However, in case of a discontinuation of ENISA without replacement, this would require additional investments by national public authorities (multiplied per each Member State) and businesses as they would not benefit any longer from 'free of charge' services (for example the trainings, the publications, the good practices, the cyber exercises) that would have to be replaced either with in-house capacity or with external contracts. A recent study shows that it is considerably less costly to carry out the tasks assigned to the agencies at the EU level than it would be if these tasks were undertaken by the EU28 Member States[116]. In the case of the replacement of ENISA with a new EU level body, the EU would incur additional set-up and operating costs, which would be as a minimum equal to the existing ones. The establishment of a new body would require additional time: a minimum estimate would be of additional three years (including one year to develop a proposal and one to two years for a new seat agreement and logistic set-up). A significant negative impact on the efficiency would derive from the loss of the current expertise of ENISA staff and economies of experience of the organisation as a whole.

Lastly, this option has not received support by any category of stakeholders. The need for an EU-level body, in particular ENISA, to improve cybersecurity across the EU has been expressed by 98% of the respondents to the public consultation on ENISA review. The opinions expressed by stakeholders across the board (Member States authorities, CSIRTs, industry, academia, EU institutions) went in the same direction during the course of the evaluation of ENISA and the other targeted consultations (CSIRTs Network survey, stakeholder workshops, Member States roundtable – see Annex 2 for more details).

- **Option 4 'ICT security internal market legislation'.** This option could significantly solve the problems identified. However, it would entail the identification or development of a cybersecurity standard that is product-specific. Extensive analysis would be needed to identify such a product. It would be also challenging to justify the selection of a specific product or sectors over others equally in need of cybersecurity assurance. Such a 'vertical' approach may be limited in light of the high variety of ICT products and services, their specific security needs and types of employment. Rather, stakeholders' consultations and technical studies suggest focusing on identifying priorities for ICT certification across sectors. Moreover, this option was discarded because it would imply a

[116] The Cost of non-agencies with relevance to the internal market, European Parliament study, 2016. The study introduces general findings and then focuses on the case of seven fully or partially self-financed agencies.

disproportionate burden and cost, especially for industry and Member States. 72% of respondents (e.g. 24) of the ENISA survey on ICT security certification (see Annex 2) indicate 'cost' as the main issue they face when dealing with security certification. SMEs in particular will bear an unduly high costs and administrative burden. Another factor that explains this choice is related to the lack of evidence as on the impact as well as on what should be the scope of such a measure (products, services, sectors, component, and systems) and capabilities across the EU. This option will require a significant mobilization of resources to monitor and ensure compliance. In addition, this approach is not flexible enough to cope with technological changes and developments taking place in a dynamic environment.

For these very reasons, this option has very little support from stakeholders. Overall, at least at this stage, this is a very ambitious and impractical option, that could however be considered in the future, as further evidence on its impact and scope becomes available.

6. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section analyses the economic, environmental and social impact of the options in line with the Better Regulation Guidelines together with the coherence with other policy and the views of stakeholders. The description of the impact of the options included in this section is complemented by the economic analyses conducted by external contractors in the context of two studies supporting the present impact assessment (see Annexes 5, 6 and 7). As the external studies make clear, the economic assessment faced some limitations in the collection of data, whose impact was mitigated to a maximum possible extent.

6.1. ENISA

Option 2 Reformed ENISA

Effectiveness
Objective 1: Increasing **capabilities and preparedness** of Member States and businesses
A **permanent mandate** would ensure that ENISA supports Member States and businesses in a sustainable manner, providing opportunities for **long term vision and planning** of the work both to the Agency and to its constituents. The partial revision of the Agency's **governance and operations** – in particular the closer involvement of the Permanent Stakeholder Group (PSG) in the definition of the work programme of the Agency – would allow the wider community of stakeholders, in particular businesses to receive better support in terms of what they really need to increase their capabilities. A very significant impact on the capabilities and preparedness of Member States is in particular expected from the provision of **long-term strategic analyses** of cyber threats and incidents. This will help identify emerging trends, provide authoritative **guidance and reports** on cybersecurity matters targetted at private organisations and citizens, assist in the **brokerage of expertise and good practices** between Member States and **provide trainings and training material** for national authorities and for CSIRTs operations, as well as guidance on **improving CSIRT maturity** according to EU and international best practices. The **reinforcement of the Cyber Europe exercises**, and the involvement in the proposed blueprint for cyber crisis cooperation (see

description of the option for more details), could help achieve one key milestone for EU preparedness which is the availability of a well-reharsed and agreed plans in case of large scale cross-border cyber incident. The involvement of ENISA in the development and implementation of EU policy on **ICT security certification** is furthermore expected to positively, although indirectly, impact EU overall preparedness. In fact, the promotion of appropriate certification guidelines supporting EU recognised schemes will not only improve the level of assurance of the security properties of ICT products and services, but it will also stimulate the uptake of adequate security standards. The impact of this policy is expected to be quite far-reaching considering the wide concerned range of stakeholders (from individual buyers to operators of critical infrastructures).

A positive impact can be inferred on the capabilities of private actors which operate within Member States and across borders, through the contribution to the establishment of **Information Sharing and Analysis Centres** (ISACs) in various sectors. ENISA would be able to provide best practices and guidance on available tools, procedures as well as support to appropriately addressing regaulatory issues related to information sharing.

Objective 2: Improving **cooperation and coordination** across Member States and the EU, institutions, agencies and bodies.

This option builds on what the evaluation identified as one of the key strenghts of ENISA – bringing Member States and, more broadly, NIS communities together for the purpose of cooperation – so it is expected to fully support the objective of improved **cooperation** across Member States and EU institutions, agencies and bodies. In particular, the support for a **harmonised approach to EU cybersecurity policy**, both upstream in the development phase and dowstream in the phase of implementation (starting with the key role the Agency can play under the NIS Directive), can signficantly contribute to increasing effective cooperation. A positive impact is also expected in terms of enhancing **cooperation within the private sector,** in particular through increased information sharing linked to the stimulation of ISACs (see above). The positive impact will moreover also cover the link **between public and private actors**, especially through the support through the establishment of research and innovation priorities in the context of the contractual public-private partnership on cybersecurity and the operational cooperation. Here an increased involvment of industry is expected, in particular regarding critical infrastructures.

The contribution to **policy development in the area of NIS** should furthermore support cooperation amongst national authorities and regulators across all sectors as part of the NIS Directive and should lead he telecoms sector to promote best practices and exchange lessons learned amongst sectors.

Furthermore, it is reasonable to assume that the clear positioning of ENISA in the EU cybersecurity ecosystem and the better definition of the links and 'bonds' with other EU institutions, agencies and bodies would result into a stronger cooperation within the EU cybersecurity ecosystem.

With respect to the aim of improved **coordination,** both across Member States and EU institutions, agencies and bodies, some activities included under option 2 are presumed to be particularly effective, in particular: the **pooling of information** on cybersecurity deriving from the EU institutions, agencies and bodies; the support to **test the blueprint** for cyber crisis cooperation; the requirement for EU and national authorities to **consult and/or take into account ENISA's opinion** when developing/implementing policies on cybersecurity; and the support for the Cooperation Group to achieve a **consistent approach to the NIS Directive implementation** across borders and sectors.

An important caveat that would influence the effectiveness of this option with regard to objective 2 is the degree of actual engagement in cooperation and coordination (besides the overall positive attitude shown in the consultation process) by both Member States and EU institutions and bodies, which otherwise can only be stimulated to a limited extent by empowering the Agency to further work in these areas.

Objective 3: Increasing **EU level capabilities to complement the action of Member**

States, in particular in the case of cross-border cyber crises.
Under this scenario, the factor of change that would significantly help meet the objective of increased EU capabilities is the provision to grant ENISA a more precise mandate on the range of the operational activities it could perform. ENISA would develop its existing **prevention** capabilities within the **cybersecurity lifecycle** (incident prevention, detection, response) and would be able, upon request and limited to pre-identified services (see description of the option for more details) to provide additional 'EU operational capacity' to complement the action of Member States. This option in fact foresees an increase in the **existing capabilities**, in particular linked to: the organisation of the pan-European cybersecurity exercises; the support to operational cooperation within the CSIRT Network, including the provision, upon Member States request, of technical assistance in case of significant incident; the funtion related to incident analysis; the involvement of ENISA in the blueprint for cyber-crisis cooperation. These tasks are expected to have a positive impact on the success of incident prevention, detection and response both at Member State and Union level. While response would remain the competence of Member States, ENISA could significantly support those Member States who would request to strenghten their own capabilities and react in case of incidents and all Member States in developing a cooperative response in case of large scale cross-border incident.
Objective 4: Increasing awareness of citizens and businesses of cybersecurity issues.
Increased cybersecurity awareness of citizens and businesses can only be achieved if all the concerned actors, from the public authorities to the individual citizens/employees, engage in the pursuit of this objectives. Uunder this option, an enhanced agency would partly contribute to this result by positioning itself as a centre of excellence for EU knowledge and information in this field. This would in fact entail a series of activities that are expected to positively impact the overall level of information and knowledge of cyber issues. It would include: the promotion and sharing of best practices from across the EU by pooling information on cybersecurity deriving from the EU and national institutions, agencies and bodies; the provision of advice, guidance and best practices for the cyber hygiene within the organisations; and the regular organisation of awareness raising campaigns in coordination with the responsible authorities in the Member States**.**
Objective 5: Increasing the overall **transparency of cybersecurity assurance** of ICT products and services in order to strengthen trust in the digital single market and in digital innovation.
Through the direct involvement of ENISA in the development and implementation of EU policy on ICT security certification, this option would contribute to achieve the objective of increasing the overall transparency of cybersecurity assurance of ICT products and services. The extent to which ENISA will be able to effectively contribute to this objective will depend on the policy approach finally taken with regard to certification, in particular whether it goes towards voluntary measures or mandatory requirements (see section 6.2).
Objective 6: Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.
Under this option, ENISA could effectively contribute to avoiding the fragmentation of certification schemes by supporting the development and mantainance of either an EU-wide scheme (as identified in section 6.2 as the extension of current SOG-IS agreement) or an EU framework for ICT security certification. In addition, linked to the possible establishment of an Expert Group (for further information see option 3 in section 6.2 below), ENISA woud help the Commission provide the secretariat of the Group.
Efficiency/Economic impact
The overall **impact on the EU economy** of reinforcing an EU agency on cybersecurity could not be estimated. Indeed, the lack of reliable detailed data and analyses related to the impact both of

increased network and information security and of cybersecurity incidents is widely acknowledged. As presented in this impact assessment, this is one of the key drivers of the problems this initiative aims to tackle. It is however possible to infer that a reinforced instrument supporting capabilities, prevention, cooperation and awareness at EU level, and therefore designed to increase overall EU cyber resilience, will have a positive economic impact by helping to reduce the costs of cybersecurity/cybercrime incidents, for which the estimated economic impact in the Union stands at 0.41% of EU GDP (i.e. around EUR 55 billion).

With regard to the **EU budget** and the overall functioning of the Agency, **efficiency gains** can be expected by the reform of the Agency. It is expected that the new set-up would help address some of the weaknesses identified in the course of the evaluation. As regards to the difficulties in recruiting and retaining highly qualified experts, this issue will be mitigated by the possibility for the Agency to offer better conditions of employment. In particular, the new tasks assigned to the Agency will increase its attractiveness in the labour market. This applies both to the permanent posts, which are considered more attractive "per se", and the posts for external staff (contract agents and seconded national experts), for which the opportunity to be involved in prestigious and specialised tasks will increase future employability (after the end of the contracts). Finally, the structural links between ENISA and CERT-EU, with the co-location of ENISA's staff dealing with operational matters with CERT-EU, that ensure that ENISA benefits from the needed additional expertise in the field of operational cooperation by leveraging the existing competences in CERT-EU.

The **costs** associated to the option of strenghtening ENISA would mostly be borne by the EU budget, while Member States would still be able to provide voluntary financial contributions to the Agency. Under this option, the current budget for ENISA (EUR 11 million) would need to be increased by about EUR 9– 12 million per year and be brought to about EUR 20- 23 million, covering the costs for about 50 additional staff members, equipment and meetings required by the new activities. In terms of staffing needs, it is estimated that 36 additional FTE would be permanent posts and 14 FTEs would be external posts (contract agents and seconded national experts) Annex 6 presents detailed breakdown of economic estimates.

It has to be noted that an increase of the EU contribution to the Agency would be accompanied by economies of scale in collecting relevant information on risks, threats and vulnerabilities and possibly in stronger operational cooperation at EU level, which would in turn benefit Member States' finances.

National public authorities and businesses are not expected to bear costs, as under this option it is foreseen that the Agency would continue to provide its services free of charges. At the other end, public and private organsiations are expected to enjoy direct and indirect economic benefits. The direct benefits would derive from the reduced investment needed in high quality commercial analyses and reports, as they could use those provided by the Agency, with the added value of receiving information, recommnedations and good practices from an independent source with an EU-wide perspective. In addition, businesses would incurr into indirect economic benefits deriving from a more harmonised policy approach to cybersecurity in the EU, in particular with regard to baseline security requirements, and the expected reduction of cyber incidents that would improve their overall competitiveness (see section below).

Impact on competiveness, competition and SMEs

Under this option, the Agency would perform several functions that could lead to increased competitiveness of the EU businesses, in particular for SMEs.

Providing adequate support to EU common policy objectives and standards for security and resilience could facilitate businesses' investments, including cross-borders. In particular, this applies to the role of facilitator in the establishment and take-up of European and international standards for risk management, and for the security of electronic products, networks and services. This focuses on the cooperation with Member States on technical areas concerning the security requirements for operators of essential services and digital service providers. A positive impact on

competitiveness would furthermore derive from support for increased resilience, by providing the advice, guidance and best practices for the security of critical infrastructures, by developing excellence in the security of the internet infrastructure, and by supporting the sectors identified in Annex II of the NIS Directive (energy, transport, health, water, banking, financial market infrastructure).

The businesses operating in the cybersecurity sector could also benefit from the information provided by the agency's function of market observatory, which would make the analyses of the main trends in the EU cybersecurity market available in order to enhance alignment of the demand and supply and thus enhance the competitiveness of the companies in the sector.

For SMEs and micro-enterprises, the access to free, high quality and independent information, analyses and recommendations can significantly releave their budgets, for which investments in cybersecurity can represent a significant burden. This particularly applies to the dissemination of good practices of cybere hygiene, since this could limit the currently high incidence of incorrect human behaviours on the overall number of incidents affecting companies. It has however to be noted that the overall positive impact on SMEs/microenterprises can be limited through linguistic barriers. Unless the agency would be able to devote an increasing part of its resources to translation services or national experts, cooperating with the agency would involve translation responsibilities, and the dissemination of material exclusively in English limits its accessibility throughout the EU.

Environmental impact

No significant environmental impact is expected for any of the objectives.

Social impact

A positive, although indirect, impact can be attained on the social sphere. As extensively presented throughout the report, cyber incidents can have far-reaching consequences for the society. The incidents related to connected devices that are increasingly represented by consumer goods used in the everyday light further exemplify the risks incurred. A reformed EU agency can contribute to achieving increased security and trust of EU citizens and businesses in the digital society. This is in particular relevant for the protection of their access to essential services, such as energy, healthcare, water, transport, as well as the security of personal data.

Coherence with other policies

Internal market – NIS policies and the Digital Single Market Strategy.

The initiative would be highly coherent with the existing and forthcoming policies, in particular in the area of the internal market. Indeed, it is designed according to the overall approach to cybersecurity, as defined by the review of the Digital Single Market Strategy, in order to complement a comprehensive set of measures, such as the review of the EU Cybersecurity Stratgey, the blueprint for cyber crisis cooperation and the initiatives to fight cybercrime. It would ensure alignement with and build on the provisions of the existing cybersecurity legislation, in particular the NIS Directive, in order to pursue further the cyber resilience of the EU through enhanced capabilities, cooperation, risk management and cyber awareness.

The overall impact on the internal market can be expected to be positive. By contributing to ensure better cooperation, more harmonised approaches to EU cybersecurity policies and increased capabilities at EU level, a more effective agency will most likely help reduce market fragmentation, build trust in digital technologies and thus reinforce the internal market.

Impacts on Fundamental Rights.

The initiative follows the main principles set out by the Cybersecurity Strategy, according to which fundamental rights are promoted and protected online in the same way and to the same extent as in the offline world.

By strengthening ENISA's expertise and support to EU policy makers, national authorities, businesses and citizens, this option is expected to help face threats such as those related to security

breaches and unauthorised access to data. It therefore promotes the safeguard of information-related rights enshrined in the Charter of Fundamental Rights, particularly the right to the protection of personal data and private life. These are highly critical issues, considering that only in 2016 about 183.4 million data records were lost or stolen in Europe due to security breaches (+93.5% in comparison to 2015).

Impacts on innovation.

This option is slated to have a positive impact on innovation. A reformed ENISA can in fact be a valuable partner for both industry and academia in the field of cybersecurity research and innovation, leveraging its practical expertise in areas such as cooperation, information sharing and regulatory requirements. In particular, under this option ENISA would support the development of Cybersecurity Research Agendas at EU and national level by providing input to the strategic analysis of trends with regard to threats, incidents and available solutions and feed into the new European Hub of Excellence in Cybersecurity, as developed in the context of the review of the Cybersecurity Strategy.

Stakeholders' support

The **vast majority of stakeholders** across all categories appear to **welcome this option**. In particular, the results of the public consultation show that ENISA is perceived by all stakeholders as having the potential to help bridge the most important gaps in the current EU by fulfilling a number of roles, such as support for: stronger cooperation between different authorities and communities; stronger EU cooperation mechanisms between MS, including at operational level; improving capacity in Member States through training and capacity building; and improving research to address cybersecurity challenges. Respondents from national authorities, in contrast to those from the industry, also specifically singled out a role for ENISA in the development of a harmonised framework for ICT security certification.

This has been further confirmed by the meetings and the interviews held with representatives of Member States' authorities and industry stakeholders. The evaluation also clearly showed that often ENISA's stakeholders express different needs which could lead to a more or less strong desire for intervention by an EU body. However, there is common agreement on the need to have (as a minimum) a well functioning agency, with a permanent mandate, which is adequately resourced and mandated to face the present and future cybersecurity challenges.

Further informaton on stakeholders' views is presented in Annex 2.

Option 3 EU cybersecurity agency with full operational capabilities

Effectiveness

Objective 1: Increasing **capabilities and preparedness** of Member States and businesses.

This option would significantly contribute to achieving the objective. In addition to the positive impacts described in Option 2, this option would increase the capacity of both Member States and the private sector to handle and respond to incidents by **providing CERT-like services**. By creating and maintaining the capacity to provide technical operational assistance to Member States CSIRTS, operators of essential services, EU bodies and institutions, the reformed ENISA could significantly step up the capabilities and preparedness of Member States and businesses.

These additional operational (responsive) capabilities can be considered a real added-value, since it would be provided to those organisations that are expressing a need and it would ensure, among the other things, that in the case of an incident or an attack, the agency can be called upon to intervene and to issue EU-level flash reports that would inform the public of the situation and, if need be, provide guidance to citizens and businesses. This would help strenghten the capabilities

of those Member States that are currently less resourced and equipped and support the more advanced Member States in gaining an EU-wide picture in crisis situations. Furthermore, in a context where organisations network and the information systems are so interconnected, bringing additional capabilities to those who are in greater need would result in an overall increased preparedness of the EU.

Objective 2: Improving **cooperation and coordination** across Member States and EU institutions, agencies and bodies.

This option would significantly contribute to achieve objective 2. The impact described for option 2 equally apply to this option. In addition, an EU cybersecurity agency with full operational capabilities is expected to achieve **increased operational cooperation and coordination**. Building on its role of secretariat of the CSIRT Network but enhanced with capacity for **real time monitoring of threats and response**, the reformed ENISA would be able to **contribute to the information exchange within the CSIRT Network**. It would maximise its output by providing real time **situational awareness reports and dynamic threat intelligence feeds accessible to all CISRTs** and, in times of crisis, to the operators of affected critical infrastructures.

Furthermore, a higher degree of coordination would be achieved, as the Agency would pool the national resources, in terms of available information, to **coordinate the operations** of the CSIRTs in case of incidents with cross-border dimension. This would avoid overlaps and maximise the possible synergies in handling the situation and mitigating its effect. In this context, there would be **full operational coordination with the EU institutions,** ensured by structural cooperation with **CERT-EU** (integration) within the context of the CSIRT Network, but also in relation to capacity building of the EU institutions (see below).

Objective 3: Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.

This option would fully meet objective 3. In fact, it would ensure that the Agency would provide the function of **European CERT**, providing all Member States and operators of essential services with support throughout the cybersecurity lifecycle - from incident prevention to response. While currently ENISA does not have CERT functions, the capacity for it could be built, for example by building on the existing competences in CERT-EU.

This approach would bring about a more radical change in the current scope of ENISA's mandate and the way operational cooperation is organised at EU level. It is expected to effectively achieve objective 3 by:

- Ensuring that the expertise and the information generated by the **operational** ('on the ground') side would **feed into strategic analysis**, the advisories and the function of facilitating enhanced EU-wide operational cooperation;
- Increasing the **overall cybersecurity capacity**, currently below the needed critical mass, and by **consolidating the competences at EU level**;
- **Granting the Member States**, with effective **ongoing hands-on support** on operational matters, in particular in terms of incident response.

In addition to option 2, under this scenario ENISA would take a **coordination role** in the implementation of the blueprint for cyber crisis cooperation.

Objective 4: Increasing **awareness** of citizens and businesses of cybersecurity issues.

This option, as presented above in option 2, will partly contribute to achieving objective 4. In addition to the impact described earlier in relation to 'Reformed ENISA', it would lead to a more effective situation awareness of citizens and businesses. In fact, the Agency would provide a service that currently does not exist at EU level, which refers to **fast information and guidanc**e in

a format accessible to the general public in the case of a signficant cross-border incident.
Objective 5: Increasing the overall **transparency of cybersecurity assurance** of ICT products and services in order to strengthen trust in the digital single market and in digital innovation.
The expected impact is the same presented for Option 2 (see above).
Objective 6: Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.
The expected impact is the same presented for Option 2 (see above).
Efficiency/Economic impact
The impact on the EU economy, as well as the one on the investment needed by public authorities and businesses, is expected to be to some extent higher than what is presented under option 2. It is possible to infer that adding more operational capabilities at EU level to complement the action of Member States can only be beneficial to the overall cyber resilience of the Union. This support would be provided to the organisations where and when it is most needed. As it has been extensively presented througout the report, an increased resilience is conducive to higher economic prosperity. This option would entail efficiency gains due to the new functioning of the Agency as presented in the previous section assessing the efficiency of option 2. The **costs** associated to the option of reforming ENISA to make it an agency with full operational capabilities would mostly be borne by the EU budget, while Member States would still be able to provide spontaneous financial contributions to the Agency. Under this option, the current budget for ENISA (EUR 11 million) would need to be increased by about EUR 17 million and be brought to about EUR 28 million. This would include the costs needed for the initial set-up of the unit providing real time threat monitoring and the set-up of the team dealing with EU-wide support for incident response. In terms of human resoources, a total of about 70 additional staff members (44 permanent posts and 26 external staff) are estimated during the start-up phase, which could further increase after some years depending on the assessment of the requests received by Member States. Further information on the analysis of the economic impact is presented in Annex 6.
Impact on SMEs, competiveness and competition
The expected impact is the same as presented for Option 2 (see above).
Environmental impact
No significant environmental impact is expected.
Social impact
The expected impact is the same as presented for Option 2 (see above).
Coherence with other policies
Internal market – NIS policies and Digital Single Market Strategy.
The expected impact is the same as presented for Option 2 (see above).
Impacts on Fundamental Rights.
The expected impact is the same as presented for Option 2 (see above).
Impacts on innovation.
The expected impact is the same as presented for Option 2 (see above).
Stakeholders' support
The **stakeholders expressed divergent views** on this option. The different needs of ENISA's stakeholders, as they emerged from the evaluation and the consultation process, lead to a lack of

consensus on whether the Agency should take on a more operational role - expanding into real time monitoring of threats and incident detection and response - or continue to remain strictly on the prevention side of the cybersecurity landscape. In particular, industry stakeholders are more positive about ENISA becoming more "hands on" in handling threats and incidents. The same applies to some Member States, in particular those that are less equipped and resourced, as they count on additional support at EU level and this could at least partially help bridge the gaps with other countries. On the other hand, the Member States that are more advanced in terms of capabilities and preparedness expressed concerns about a more radical transformation of the Agency. This departs from a model of the cybersecurity agency with full operational capabilities which is increasingly used at national level, but which is not deemed appropriate for ENISA due to, among the other things, the possible overlaps with the mission of national agencies.

Further informaton on stakeholders' views is presented in Annex 2.

6.2. Certification

Option 1: Non-legislative ("soft law") measures

Effectiveness
Objective 1: Increasing **capabilities and preparedness** of Member States and businesses.
Under this option, voluntary activites related to certification may be promoted intermittently. This may produce some positive impact on the increase of cyber resilience in the EU, but in a limited and indirect manner. Option 1 would provide a low incentive to invest resources to developing relevant expertise and facilities (e.g. conformity assessment bodies) - which involve high economic impact. In light of the fast-moving threat landscape and increased complexity of attacks, this option would have a detrimental effects on the capabilities and level of preparedness of Member States, business and critical infrastructure, which would remain uneven. In the case of co-regulation, there is a risk that the entrusted market operator may decide to promote new certification schemes that are designed to minimise its costs of compliance rather than to satisfy a public need for better ICT security. In addition, co-regulation may not be a viable political option given the high sensitivity that Member States attach to issues such as of security of their critical infrastructures.
Objective 2: Improving **cooperation and coordination** across Member States and EU institutions, agencies and bodies.
In the absence of an institutional mechanism fostering a European approach on the policy priorities in this field, Member States are likely to generate uncordinated approaches to certification . In addition, cooperation and coordination would be undermined as Member States are likely to promote their national scheme and boost its reputation. This may trigger competition among similar national schemes with Member States failing to accept certificates from foreign or private schemes.
Objective 3: Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.
This option will not produce any sigificant impact to increase EU level capabilities that complement the actions of Member States.
Objective 4: Increasing awareness of citizens and businesses of cybersecurity issues.
A soft-law approach may offer quick and cost-effective ways to embark on cybersecurity certification. This can incentivise businesses to resort to certification as a way to make customers and citizens aware of cybersecurity threats and solutions. Public authorities can lend support and encourage this approach, therefore strengthening overall awareness levels. This option may

however at the same time, have some negative impact on reaching this objective. Due to their flexibility, the soft laws instruments envisaged in this option would not act as a deterrent to the proliferation of schemes and standards. As a result, **businesses** and **end-users** (e.g. operators of critical infrastructures and citizens) may still be in a situation where multiple schemes or standards exist. Such a variety engenders lack of readability and comparability, meaning that these actors will face difficulties to judge which scheme or standard would best satisfy their particular requirements. This would increase the risk that these actors use inappropriate products or services, thus lowering the level of security of their operations.

Similarly, the development of a EU scheme through soft law would materialize on condition that public authorities, vendors and operators are highly committed and ready to mobilize resources. It is generally expected a long period of time for these conditions to occurr and thus for a EU scheme to emerge. As a result, only few products and services certified according to a EU schemes would be available on the market for end-users (citizens and operator of critical infrastructures).

Objective 5: Increasing the overall **transparency of cybersecurity assurance** of ICT products and services so as to strengthen trust in the digital single market and in digital innovation.

While the soft measures identified in this option may to a certain extent contribute to improving the current lack of overall transparency of information of ICT products and services, they also present a number of limitations. Essential elements of certification schemes would not be binding and would therefore only act as best practice recommendations. Similarly, self-regulatory initiatives tipically lack legal regulatory oversight and regular monitoring systems. This circumstance increases the risks of deceptive behaviours, that can ultimately undermine the trust in and effectiveness of these type of initiatives.

European Commission support, coordination and encouragement of industry-driven initiatives is indeed expected to help private operators in their effort to establish schemes. However, the success of these initiatives depends on the goodwill and agreement of the participating stakeholders. In addition, negotiations among stakeholders may occurr on an ad-hoc basis, may take considerable time, or may fail, while there is no guarantee that newly established schemes are widely accepted across national authorities. All self and co-regulatory efforts would necessarily follow a piecemeal approach rather than a well defined strategic design, and could entail a cumbersome and resource-intensive process. This option may therefore cause a low incentive to embark on voluntary activites, with detrimental effect on the overall need for more transparency of information on the cybersecurity of ICT products and services.

Research and raising awareness in the field of ICT certification would be very helpful as a collateral measure, but would not fully address per se the main issue of the lack of transparency on the security assurance levels of ICT products and services.

Objective 6: Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across Member States and sectors.

Under this option, the existing national certification schemes will still use different procedures, unless Member States agree on ad hoc mutual recognition agreements. In addition, sectorial certification initiatives are expected to proliferate, as the need to ensure cybersecurity becomes more pressing across sectors. This would lead to a possible scenario of a twofold fragmentation across Member States and sectors. Such a fragmentation is also likely to persist as each MS would continue to use and improve its national scheme; thus creating a strong legacy and reluctance to adopt equivalent schemes from other Member States.

The effects of this uncoordinated proliferation of multiple approaches to cybersecurity certification are likely to be that **vendors** as well as **consumers and end-users** making cross-border purchases will not necessarily be able to compare and understand the security properties of the devices purchased.

Efficiency/Economic impact

The Commission would need to bear costs related to the implementation of the measures proposed under this Option: e.g. bear costs to issue guidance, follow the standardisation efforts, facilitate self / industry led-initiatives to the extent possible, and launch awareness raising campaigns. It is estimated that this would require two administrators and one assistant working full time on these matters (running cost).

The launching of an awareness raising campaign may require the help of an external contractor or EU agency such as ENISA. The cost may be estimated in the region of EUR 250-400,000 depending on the tools employed (one-off cost).[117] The funding of projects under the CEF may be dedicated to upgrade exisitng testing facilities or building new ones.

National authorities should be involved in the co-regulatory efforts on a voluntary basis. This cost would vary according to the number of meetings and the degree of cooperation. Assuming that many issues may be steered by the Commission (e.g. a conservative estimate of three meetings a year for three years), the cost may be estimated to be between EUR 2,500 and 7,000 per authority/per annum (running cost)[118]. Similarly, national authorities would need to finance participation in efforts towards coordinated enforcement. Assuming in this case two meetings per year, the annual cost would be between EUR 1,700 and 4,700 (running cost). Minimal compliance costs for Member States' authorities to get familiar with the new implementing/soft law measures would be around EUR 1,000 per authority (1 day of training) (one-off cost)[119].

Businesses would benefit from a fast and cost-effective approach for the development of voluntary tools. A soft law approach would also imply a higher level of engagement and greater influence of business in the process of developing tools (e.g. guidelines, certification schemes etc) that better suit market sensitivities. As such, this may produce an incentive for industry to resort to ICT certification as a way to improving the quality of their products and possibly increasing their market share. However, industry will incur some costs for the participation in activities, such as establishing codes of conduct and standard-setting etc. Considering past similar exercises, it could be assumed that the increase of cost would be moderate, as participation would be voluntary and normally only a relatively small proportion of businesses participate in such activities (running cost for the duration of the standardisation activities). Indeed, some businesses already participate in such activities[120]. Businesses would be more extensively affected by the specification of EU standards, to the extent that they would implement the new standards (one-off cost and lower running cost ensuring updates). Depending on the content of such standards, companies concerned may be more significantly affected. However, the implementation of such standards will essentially depend on the decision of each and every firm (i.e. it will be voluntary). Therefore, it is not possible to provide a clear and precise estimate of the magnitude of the impact. Some cost savings (especially for industry already subject to certification requirements) would occur if a EU-wide certification schemes in specific sectors is established. This would enable industry to certify their products and services only once and against a scheme that is recognised in the whole of the EU. However, given the voluntary nature of this option and the absence of a formal governance structure for ICT certification in the EU, industry will have to invest significant resources (both human and financial) to reach consensus among various actors (both private and national) on the development of a ICT certification scheme that is widely accepted across Member States.

In conclusion, this option presents moderate/low implementation costs for the Commission and

[117] This means that costs will be lower in case e.g. only an online campaign would be launched. In case e.g. an EU-wide awareness-raising campaign is launched with printed materials, informative events, discussion rounds etc., the costs will of course be higher than this estimate.

[118] This is based on the assumption that between one and two persons per MS might join, that they need to spend time on travel, the meeting itself and preparation considering the hourly salary quoted by the Commission and that they need to pay for flight and in some cases for one night accommodation.

[119] Familiarisation/training costs= 3 staff-members per authority needing training * hours spent on training per staff (8 hours) *staff costs per hour (hourly wage rate EUR 41.5, Eurostat data 2012).

[120] Examples ares the cloud computing group and the C-ITS group.

Member States. In particular, the weak benefits/cost savings for businesses in Option 1 would indeed materialize, but only after a successful complition of a scheme. However, such a process would imply additional costs and generate some inefficient allocation of resources. At the same time, the dissemination of additional guidance may contribute to enhance legal certainty.

Impact on SMEs, competiveness and competition

The impact on SMEs under this option would depend on their willingness to participate in the development of guidelines, certification schemes, standards and best practices recognized across Member States.
SMEs and microenterprises already subject to ICT security certification requirements would have a significant interest in following these voluntary activities. Possible outcomes of soft law activites may improve SME's access to markets. However, contrary to larger businesses, these actors typically have limited budgets. Unless they are willing to bear the costs deriving from participation, microenterprises and SMEs would be mere recipients of the outcome of voluntary initiatives. This implies that they need to understand and apply new guidelines and standards developed by other actors. In addition, under this option any initiative or proposed processes for security certification will be defined without paying attention to the needs of SMEs, with unfavourable effects on their competitiveness.

Environmental impact

No significant environmental impact is expected for any of the objectives.

Social impact

To the extent that multiple certification schemes remain in place and the process of developing new European schemes is uncoordinated, the incentive to encourage ICT certification will be low. As a consequence, this option would provide limited support to mitigate the current asymmetry of information among various stakeholders (e.g. **manufacturers, operator of critical infrastructure, citizens**) and foster trust in the Digital Single Market. In particular, ad hoc voluntary initiatives promoted by the Commission would provide limited support to increase the level of assurance of critical infrastructures. Operators would not be able to rely on an institutional framework to express their need for more security, rather they will have to bear the burden of gathering consensus among vendors and national authorities.

Coherence with other policies

Internal market – NIS policies, digital single market, trade.

The impact on the internal market may be considered mildly positive. Interpretative communications from the Commission, self and co-regulation initiatives, as well as standardisation activity at EU level would contribute to a certain extent to greater harmonisation and to reducing fragmentation. International trade is promoted to the extent that these voluntary activities adhere to internationally recognized standards.

However, there are also important limitations to the harmonising effects that these measures could achieve. The development of private and national schemes will not be discouraged, leading to detrimental effects on the digital single market. In addition, as measures are not binding, it will rest ultimately on the national authorities and buyers whether or not to propagate the usage of these schemes/measures. Moreover, the success of self-regulatory measures depends on a number of circumstances, such as the degree of participation and compliance by the industry concerned. Finally, since the use of IT certification would not be directly promoted, this option would not help reduce the risk that Member States set different security requirements to demonstrate compliance with the NIS Directive.

Impacts on Fundamental Rights.

To the extent that ICT security certification will contribute to increase cybersecurity online, these proposed actions will produce a mild increase in the protection of fundamental rights, such as rights to privacy, data protection, security and life.

Impacts on innovation.
To the extent that it raises funding for R&D activities in the field of security research and that it encourages the establishment of industry initatives promoting cyber-certified security solutions, **Option 1** is slated to have a positive impact on innovation.
Stakeholders' support
The majority of stakeholders would welcome soft-law initiatives and Commission support to industry-driven initiatives across all categories. However, they are also widely convinced that, in the absence of an overarching European legal framework for certification , these types of initiatives would not by themselves be sufficient to significantly discourage the proliferation of certification schemes and would not increase transparency. Member States have also stressed the risk that providers of essential services operating cross-border could be subject to different security requirements in relation to IT certification.

Option 2: EU legislative act to create a mandatory system for all Member States based on SOG-IS.

Effectiveness
Objective 1: Increasing **capabilities and preparedness** of Member States and businesses.
This option would provide Member States with an institutional fora, enabling all Member States to express their security needs related to certification. As a result, Option 2 is expected to help Member States improve their capacity and preparedness, thus generating an overall positive effect on the cybersecurity resilience in the EU. The SOG-IS MRA community gathers national officials from 12 Member States plus Norway with long-standing expertise in the field of IT security. As such, new members – who will be required to join SOG-IS MRA - are enabled to gain relevant competence in this area. However, any concrete action to increase both capabilities and level of preparedness remains at discretion of each Member State. In addition, it is important to note that new members are expected to join the SOG-IS MRA as 'certificate consumers' from the outset, with a view to becoming a 'certificate producers' once adequate expertise and facilities will be built. Once again, such a decision would be voluntary. In addition, the impact of this option on level of capabilities and preparedness of critical infrastructures may depend on the extent to which Member States decide to foster the use of SOG-IS-certified products (e.g. through public procurement) for the operation of critical infrastructures in their territory. For business, the positive impact on their capabilities and preparedness will highly depend on their level of commitment to adopt the certification methodology promoted under the new SOG-IS MRA.
Objective 2: Improving **cooperation and coordination** across Member States and EU institutions, agencies and bodies.
This option would improve cooperation and coordination among Member States within its product scope, since it provides an institutional mechanism that enables exchange of information and consensus on the policy priorities in the field of security certification. However, in line with the experience of the current SOG-IS MRA, cooperation and coordination may be limited to high level product certification. National and uncordinated approaches can still proliferate for a wide range of products and services requiring medium to low level of assurance. This is already happening in countries which are members of the SOG-IS MRA. Examples of national schemes include: CSPN in France, CPA in UK and a baseline scheme in Germany. Currently, these schemes are not mutually recognised. ENISA would help run the Secretariat of the EU-wide SOG-IS. The choice of ENISA for this role is consistent with the need to ensure cooperation and coordination in the area of

cybersecurity (see Option 3, section on effectiveness, for analysis of alternative to ENISA).

Objective 3: Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.

This option would mildly help meet this objective, to the extent that all Member States agree on the creation of capabilities for certification at EU level. However, this could only be envisaged in the long term. Initiatilly, Member States would be simply encouraged to improve their national capabilities.

Objective 4: Increasing awareness of citizens and businesses of cybersecurity issues.

The current SOG-IS MRA has to date undertaken only limited awareness raising activities. This situation is likely to remain unchanged if the MRA is extended to all Member States, unless Member States specifically allocate budget for these activities.

Objective 5: Increasing the overall **transparency of cybersecurity assurance** of ICT products and services so as to strengthen trust in the digital single market and in digital innovation.

Option 2 would partially contribute to achieve this objective. The SOG-IS MRA, which relies on the testing methodology of CC[121], has been used to certify only a few digital products requiring high level of assurance (e.g. tachographs, digital signatures and smart cards). This is due to the depth of the evaluation[122] of CC, which generates high costs, and lengthy processes. As such, the CC methodology used by SOG-IS MRA is unsuitable for the security certification of products requiring medium and low level of assurances.

It is therefore expected that this option would foster transparent information only for products requiring high levels of assurance. In addition, there will not be an increase of transparency of cybersecurity of ICT services as the current CC methodology is only suitable for the security certification of products.

Objective 6: Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.

Option 2 would partially contribute to achieving the objective. The creation of a mandatory system for all Member States under the SOG-IS agreement would imply that certificates issued under the extended SOG-IS MRA would be recognised in all Member States and not only in the 13 members of the current SOG-IS MRA. However, as SOG-IS certificates are used for products (not services) requiring high level of assurance, the proliferation of national schemes to certify commercial products as well as services – normally requring a low level of assurance - can still be expected. If not addressed, each Member State would continue to use and improve its national scheme for low levels of assurance; therefore creating a strong legacy and reluctance to adopt equivalent schemes from other Member States.

As previously explained, this is already happening in countries which are members of the SOG-IS MRA. Examples are: CSPN in France, CPA in UK and a baseline scheme in Germany. Currently, these schemes are not mutually recognised.

This scenario is expected to worsen as the demand for some form of IT security covering also commercial products and services grows worldwide.

Overall, the positive impact of Option 2 in solving fragmentation is potentially significant, but limited to high level certification. Not only national schemes for medium, and low level of assurance can proliferate outside the extended SOG-IS MRA, but they can also compete. In this last scenario, Member States may have a little incentive to turn to the mutual recognition of a similar, competing scheme.

[121] For an overview of criticism related to CC, see JRC study Annex 8, pp. 24-26.

[122] The CC methodology is based on third-party evaluation for all its 7 levels of assurances. As such it does not envisage self-evaluation.

Efficiency/economic impact
The costs for the **Commission** are not very high and essentially coincide with the legislative process. The Commission would have to invest resources to oversee the implementation and extension of the current SOG-IS MRA. It is estimated that this would require two administrators and one assistant working full time on these matters (running cost). **Member States** will have to implement the new rules. The 13 Member States which are already members of the SOG-IS will not have to bear any significant additional cost. Costs will be more significant for those Member States that are not currently members. According to the the data produced by the Interim Report of the technical study, the costs of participation in the SOG-IS MRA for a Certification Authority are approximately EUR 58,000. This includes the participation in Management Committee meetings (1-2 times per year) and the JIWG meetings (3-4 times per year). It also includes yearly travelling costs for three members attending six meetings, the preparation of meetings, attendance and national reporting. Other costs are related to the start-up of an IT certification (e.g. process setup, development and accreditation of evaluation facilities, institutional communication). However, it should be considered that the SOG-IS MRA provides the possibility for its members to act as certificate 'consumers'[123] as well as certificate 'producers'[124]. Consumers would be able to benefit from a situation in which they simply accept certificates issued from producers, and will have little incentive to invest resources to build the appropriate facilities and expertise to become a producer. As a consequence, existing producing members may face a raise in the demand for certification which will trigger the need for an economic investment aiming to upgrade the existing facilities. However, producers would gain more expertise to set priorities and shape the course of IT security certification in Europe. Conversely, new members of the SOG-IS are expected to join as consumers in order to avoid upfront investment costs related to capacity building and training. As such they would have little incentive to build extensive expertise. This Option would not imply significant additional costs for **industry**, namely because security certification will remain essentially a voluntary tool. As it is the case today, businesses will remain free to choose whether to certify their products. By contrast, whenever a SOG-IS certificate will be required (e.g. public procurement), business would benefit from a EU-wide mechanism. This would certainly act as a cost-reductor especially for those firms that already use SOG-IS certificates.
Impact on SMEs, competiveness and competition
Option 2 may have a positive effect on SMEs that already rely on the SOG-IS mechanism as they can use certificates throughout the entire EU. In addition, this option may provide an incentive for those SMEs willing to certify their products, as they can rely on such an EU-wide mechanism. However, these positive effects are limited due to the shortcomings of the current SOG-IS MRA (e.g. fit for high level of assurance, duration of process and costs). SMEs would likely not have the resources to go through such a time-consuming and potentially expensive process. It is therefore reasonable to expect that the competitiveness gains will not very high for market operators.
Environmental impact
No significant environmental impact is expected.
Social impact
This option would increase the security of our critical infrastructures. Member States may wish

[123] E.g. national authorities accepting certificates issued by other authorities who are members of the SOG-IS MRA.

[124] E.g. national authorities issuing and accepting certificates from other authority's members of the SOG-IS MRA.

to include SOG-IS certificates in public procurements requirements, with a view to enhance the assurance level of critical infrastructres. For their part, vendors would be able to certify their products by relying on a one-stop shop mechanism. This would foster a chain of trust among vendors and operators of critical infrastructures. However, asymmetry of information would persist between vendors and citizens for commercial products requiring medium to low level of assurance.

Coherence with other policies

Internal market - NIS policies and digital single market, trade and international aspects

Option 2 would have a positive effect on the internal market. The measures at stake would cover some gaps of the existing European certification landscape, partially solving the problems related to its lack of transparency, inconsistency and fragmention. Accordingly, the option is expected to slightly or moderately enhance harmonisation of certification requirements in the digital single market. The increased cooperation may foster consistency across Member States and possibly promote a common use of ICT certification as a way to demonstrate compliance with the NIS directive. Finally, as the CC methodology relies on an international standard, this option would be aligned with the terms of international trade. This effect is however limited to products requiring high level of assurance.

Option 2 would also lead to a strengthened European position in the international context, and may become a model for other world's regions.

Impacts on Fundamental Rights

To the extent that ICT certification will contribute to increase cybersecurity online, these proposed actions will also increase the protection of fundamental rights such as rights to privacy, data protection, security and life.

Impacts on innovation

As the constrainsts of the current SOG-IS would be transferred to its upgraded EU-wide version (e.g. fit for high level of assurance; focus on products rather than services), firms may not consider the extended SOG-IS MRA as a suitable tool to ensure the cybersecurity of their innovative commercial products and services requiring a low level of assurance. They would rather look for more agile (national or private) certification schemes. However, as these schemes are usually used within national boundaries and may not be widely accepted, there would be an incentive to avoid ICT certification in order to cut administrative costs related to multiple certification processes.

Stakeholders' support

While stakeholders generally praise the work of SOG-IS MRA and are willing to see SOG-IS scheme thrive in the future as a tool of mutual recognition based on internationally recognised standards (e.g. CC), the majority of stakeholders (especially Member States and industry) are aware of the limitations of the current SOG-IS MRA and therefore consider that a significant adaptation and upgrades would be needed.

Option 3: EU general ICT security certification framework

Effectiveness

Objective 1: Increasing **capabilities and preparedness** of Member States and businesses

Procedures for security certification would be simplified through an EU-wide framework leading to mutual recognition of certificates issued under a European cybersecurity certification scheme. This would provide a strong incentive for Member States and operators of essential services to increasingly resort to security certification (e.g. through public procurements) as a tool to reduce

the vulnerability of critical infrastructures and increase their preparedness.

Rules are simplified and certificates will be valid across Member States. This will incentivise businesses (especially those with cross-border operations and digital service providers) to use security certification as a way to increase preparedness of their operations.

Objective 2: Improving **cooperation and coordination** across Member States and EU institutions, agencies and bodies.

This option would improve cooperation among Member States, since it provides an institutional framework that enables the development of European cybersecurity certification schemes and the development of a common policy in this crucial field. National and uncoordinated approaches in this field would be highly discouraged. Contrary to Option 2, such a positive effect is expected to cover products as well as services at all levels of assurance (high, medium, low). However, the use of European schemes may vary across Member States. For example, some may resort to European schemes to better protect a critical infrastructure while other may not. In an interconnected digital market, this scenario increases the risk of vulnerability and proliferation of threats, even in those Member States adopting higher level of protection through certification. It is therefore expected that, Member States not adequately using certification schemes would face pressure to align with those that do.

Moreover, assigning a role to ENISA in the area of ICT security certification is consistent with the need to ensure cooperation and coordination in the area of cybersecurity. Over the years, the Agency has acquired significant expertise in the area of security certification and standardisation. It has engaged with private sector, notably providers of cybersecurity products and solutions by means of workshops and targeted surveys. It has established channels of dialogue with the national certification bodies and standardisation bodies through participation in the Management Committee meetings of the current SOG-IS MRA and it is in regular contact with the Cybersecurity Coordination Group created by CEN CENELEC and ETSI. The Agency has also authored a number of technical studies on certification and standardisation. In particular, in the area of cloud computing certification, ENISA has developed a meta-framework, which maps the security requirements in existing cloud certification schemes[125].

DG JRC has been considered as an alternative to ENISA. DG JRC has considerable expertise in this area since it currently hosts testing laboratories for certification of digital tachographs and has published a number of studies that have informed this initiative, among others. However, stakeholders' consultations suggest that JRC's unique technical competence in relation to cybersecurity would be best utilized in support to EU's endeavours in research and development, which are necessary to keep pace with the dynamic nature of digital security. For example, JRC may explore more efficient testing methodologies to carry out ICT security certification. Moreover, resorting to JRC as an alternative to ENISA may be discarded on the ground of political considerations. As security certification may interfere with sensitive areas, national authorities may resist the option of conferring a coordination role to a Commission DG.

Objective 3: Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.

If needs arise and on condition that financial resources are available in the future, a specialized European testing laboratory supervised by ENISA could be built to support the capabilities of Member States lacking such facilities. A future European laboratory may also act as a centre of

[125] The Commission has already used the outcome of this project in a large cloud services procurement tender (2500 cloud virtual machines and 2500 Terabyte of cloud storage), which builds upon the 27 security objectives identified in the meta-framework.

competence to conduct experiments with a view to advance the state-of-the-art in the field of security certification.

Objective 4: Increasing awareness of citizens and businesses of cybersecurity issues.

ENISA would be tasked with activities related to communication and dissemination of best practices and raising awareness in the field of cybersecurity certification. ENISA has acquired extensive experience in this type of activities and is bound to further reinforce its role and resources in this area. This option would, therefore, greatly improve the awareness of citizens and businesses of cybersecurity issues.

Objective 5: Increasing the overall **transparency of cybersecurity assurance** of ICT products and services so as to strengthen trust in the digital single market and in digital innovation.

Option 3 would partially contribute to achieve this objective. Similarly to the other options presented in this section, in the absence of mandatory requirement to certify, the creation of a framework alone does not have a direct effect on the increase in transparency of cybersecurity assurance of ICT products and services. Nevertheless, a European certification framework increases the value of security certificates as they can be used across Member States through a single process. This creates an incentive for vendors to embark on such a process with a view to increase the quality, and market share of their innovative products and services without the administrative costs of multiple processes. In this respect, initiatives such as the IoT trust label, which aims to satisfy the need for more transparency, would normally fit within the scope of such a framework.

This option would also enable operators of essential services to have more information on the security properties of the digital devices used in their infrastructures, by undergoing the relevant certification procedures for their products and services in accordance with European scheme,

Objective 6: Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.

Option 3 would highly contribute to achieving this objective. This Option would remove the possibility of coexistence of national certification schemes for products and services covered by a European scheme and make the creation of private outside of the future European certification framework significantly less attractive. Certificates issued from schemes outside the framework would face acceptance problems. Similarly, the creation of national schemes remains possible, but limited to national security, which is a narrow and sensitive area. For this reason, these national schemes are expected not to interfere with future EU schemes under the framework, that would be mainly designed for improving the security of the digital single market.

Efficiency/economic impact

The costs for the **EU** instituions, **ENISA** and **Member States** coincide with the establishment and maintenance of this European Framework. In particular, the European Commission would have to place resources to support the establishment of the framework, notably for the adoption of the European schemes by means of delegated acts or implementing acts. It is estimated that this would require three FTEs working full time basis (e.g.two administrators and one assistant)

The EU institutions would also bear the costs related to the set up of the Expert Group. Typically, the Commission allocates 600 Euro per expert who will qualify for travel reimbursement. Since each Member State will appoint a representative, the total cost of the group is estimated to be in the region of 16,000 - 17,000 Euro per year.

ENISA is expected to bear the bulk of the costs related to both the functioning and maintenance of the framework, as it will be in charge of a) preparing the candidate schemes and b) issuing

guidelines and c) help the Commission provide the secretariat for the Group. The instituional costs related to ENISA are included in the economic estimates for ENISA (see Annex 6).

As an alternative to ENISA, it has been estimated that establishing a new body with the appropriate expertise in such a complex area would take between 5-7 years. Approximately, the costs of setting up a new European body amount to EUR 21,9 million. ENISA as the EU agency for cybersecurity with strong links with Member States has been considered to be best placed to ensure a coordinated and efficient approach to any European effort on security certification, for example by bringing all relevant stakeholders together, coordinating their work on certification schemes, preparing certification schemes and provide technical expertise.

Member States appointing a competent certification authority are expected to bear costs that would approximately amount to 1,600,000 Euro per year[126]. This estimate include costs related to personel, equipment, subcontracting, operations (incl. training conferences) as well as set up of evaluation facilities. The operational management of a certification authority would also require investments for carrying out enforcement and supervision activities. Costs related to these activities are in the region of 290,000-300,000 Euro (per year) Generally, the overall impact will be significantly lower (or neutral) on Member States that are already part of the SOG-IS MRA and that have a supervision authority already in place.

This Option would not impose additional costs for the industry in the short term, namely because certification will remain essentially a voluntary tool. As is the case today, businesses will remain free to choose whether to certify their products or services. By contrast, the possibility to obtain an EU wide certificate would certainly act as a cost reductor for those firms that already certify their products or as an incentive for those that are willing to do so.

Since the certification process involved in future European schemes would depend on the associated level of assurance, cost and duration would be reduced compared to the current SOG-IS MRA, built on the lenghty and complex CC methodology.

Impact on SMEs, competiveness and competition

Option 3 would have a very positive effect on competitiveness, as it would significantly reduce costs and administrative burden for SMEs that already certify or are willing to certify their products and services at various level of assurance. This option would also eliminate a potential market-entry barrier (for both new business and SMEs) and enable access to a wider cybersecurity market.

The mutual recognition mechanism would also boost the competitiveness of firms operating cross-borders, by providing an incentive to certify their products and thus help them reap the advantages of increased trust in the digital solutions and gaining access to market segments where certification is required (e.g. some areas of public procurement).

In addition, this option would foster expertise in the field of IT certification, in particular among the business community operating in Europe. A security-by-design approach also for mass products and services would be encouraged as a consequence. Since the demand for more secure solutions is expected to raise worldwide, industry (incl. SMEs) operating under the European framework would enjoy a competitive advantage to satisfy such a need, therefore potentially gaining shares in the global market.

Environmental impact

No significant environmental impact is expected.

[126] Approximately amount for the first 3 years. More detailscan be found in the support study (Annex 7)

Social impact
Certification of products and services at various level of assurances will enable end-users to make more informed purchase decisions. This would also help maintain a chain of trust among various stakeholders - from the manufacturer to the operator of critical infrastructure up to the final end-user (public authorities, citizens). The current asymmetry of information would be reduced. In particular, this option would enhance the level of assurance of critical infrastructures, since operators would have an institutional structure to express their need for ICT certification.
Coherence with other policies
Internal market – NIS policies, digital single market, trade and international aspects
Option 3 would have a positive effect on the internal market. The measures at stake would address the potential fragmentation caused by existing and emerging national certification schemes, therefore contributing to the development of the digital single market. Accordingly, this option is expected to promote convergence on the creation of new European certification schemes whenever a need arises, thus addressing the risk of multiple approaches across Member States. Moreover, this option supports and complements the implementation of the NIS Directive by providing the undertakings subject to the Directive with a tool to demonstrate compliance with the NIS requirements in the whole Union. In developing new cybersecurity certification schemes, the Commission an ENISA should pay particular attention to the need to ensure that NIS requirements are reflected in the certification schemes. The undertakings subject to the NIS rules may thus use certificates issued under the European schemes as an element to be taken into to demonstrate their compliance with the NIS Directive. Under this option, the functioning of the European ICT security certification framework will be designed to ensure full coherence with the General Data Protection Regulation(GDPR)[127] and in particular with the relevant provisions on regarding certification[128] as they apply to the security of the processing of personal data. An EU level ICT security certification framework which is proportionate and wherever possible based on international standards would significantly contribute to an international trade-friendly level playing field for products and services. To the greatest extent possible the schemes proposed in the future European framework would rely on international standards as a way to avoid creating trade barriers and ensure coherence with international initiatives. For example, the current SOG-IS MRA, which coordinates the standardisation of the international Common Criteria methodology among its European members, is likely to be included in the future Framework as the European scheme for high level certification. In addition, a European framework will support the coordination of certification policies among European certification bodies, thus promoting a common position in the international CCRA ,
Impacts on Fundamental Rights.
To the extent that ICT certification will contribute to increasing cybersecurity online, these proposed actions will also increase the protection of fundamental rights such as rights to privacy, data protection, security and life.

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

[128] Such as Articles 42 (Certification) and 43 (Certification Bodies) as well as Articles 57, 58, and 70 regarding respectively the relevant tasks and powers of the independent supervisory authorities and the tasks of the European Data Protection Board.

Impacts on innovation.
Option 3 would promote the production of innovative, more secure, digital solutions for which a high demand is expected globally. The development of an innovative solution may not be sufficient to acquire market shares if its cybersecurity is neglected. For example, Fabasoft (an innovative Austrian SME) has used security certification[129] to build its credibility as provider of secure eGov solutions, and gain access to other markets (Germany) through public procurements[130] Furthermore, the cooperation between ENISA and standardisation bodies would enable to monitor the appropriateness of standards used in a European scheme so that they ensure an adequate level of both security and technological innovation. Such a monitoring exercise would mitigate the risks related to the obsolescence of standards that may provide buyers with a a false sense of security.
Stakeholders' support
The majority of stakeholders are in favour of the creation of a voluntary, scalable European framework based on a mutual recognition of certificates, and including all Member States. However, representatives from industry and national authorities have stressed the necessity to provide adequate staff in order to support the functionning of this Framework. For this purpose, it was suggested that ENISA, among other tasks, helps carry out secretarial tasks.

7. HOW DO THE OPTIONS COMPARE?

This section presents a comparison of the options in the light of the impacts identified. The options are assessed against the three core criteria of effectiveness, efficiency and coherence, as well as taking into account the support expressed by the different stakeholders.

ENISA

Table 5 below presents a comparison of the options based on the analysis of the options 0 and 1 and the detailed assessment of the options 2 and 3. The comparison is mostly based on a qualitative analysis, while quantitative data support the assessment of the economic impact and efficiency. With regard to this criterion, it is assessed the expected impact on the EU economy as well as the financial implications for the EU budget. As stressed since the beginning of this report, **the impacts of the options for the future of ENISA cannot be considered as generated exclusively by the Agency**, as **no entity can have a standalone impact** in cybersecurity. Therefore, the effort here made is to focus as much as possible on the impact that can be attributed to the Agency, while taking into account the contextual elements and the other known instruments.

Having regard to the **effectiveness**, it appears that both option 0 (baseline) and option 1 (expiry of ENISA mandate) would not be able to achieve the objectives of the initiative which call for increased capabilities, cooperation, transparency and reduced fragmentation. With respect to the baseline, both option 2 and 3 are clearly more effective. A 'Reformed ENISA', which builds on the NIS Directive, including in terms of

[129] A list of security certificates acquired by Fabasoft are available here: https://www.fabasoft.com/en/group/transparency/certifications-audits

[130] Certification is obviously not the only criteria taken into account, but fostered a reassurance that Fabasoft innovative solutions are also secure.

operational cooperation, and the key strengths highlighted in the evaluation (such as the cyber exercises and the community building) and provides support in such a key area for the market as security certification for ICT products, is expected to effectively contribute to most objectives. Option 3 is deemed more effective than both baseline and option 2 in relation to meeting the objective of increasing EU level capabilities to support Member States and the overall preparedness of the EU, especially in times of crisis.

The **economic impact** of option 0 and option 1 is deemed to be negative. Under the baseline scenario, ENISA would continue for a fixed number of years to receive funding from the EU budget – which being rather small in comparison to the investment in other agencies can be judged as 'efficient' – but with its current mandate and resources would not be able to properly support Member States, EU institutions and businesses, with indirect negative consequences on the economy. In comparison to the baseline, both option **2** and **3** bear advantages. A 'Reformed ENISA' is expected to bring positive effects for the cyber resilience and the internal market while still staying an agile organisation which would require a financial contribution from the EU higher than it is currently the case but still fairly below other agencies that also operate in critical areas (in the range of about EUR 23 million per year). The option 3 is expected to have further reaching economic benefits than option 2 (and the baseline) because the Agency would be able to provide an extra operational help to both Member States and operators of critical infrastructures. At the other end, the option of a cybersecurity agency with full operational capabilities would put higher pressure on the EU budget (associated costs estimated at about EUR 28 million per year, including the costs needed for the initial set-up). Both option 2 and option 3 are still considered efficient as potentially conducive of 'high value for money'.

In terms of **social impact**, option 1 is expected to have negative consequences in comparison to the baseline, while option 2 and 3, as presented earlier can provide increasing level of cyber resilience and thus positively impact the social sphere.

According to the criterion of **coherence,** option 1 would have a negative impact because it would imply reducing the EU effort in cybersecurity, while option 0 is considered moderately incoherent with NIS policy, because a fixed term mandate (in contrast to the tasks conferred to ENISA by the NIS Directive) and no update to the tasks/resources to match the new needs would not be consistent with the EU priorities set in the Cybersecurity Strategy and the Digital Single Market. Option 2 and 3 are both positively assessed against this criterion, as completely aligned to the objectives of EU policy.

The impact assessment exercise has shown that among all options the **stakeholders favour option 2** the most**.** There is in fact widespread consensus that an EU cybersecurity agency is needed and that the current ENISA (baseline) does not fulfil the conditions to exercise the roles that are needed and to face the present and future cybersecurity challenges, but that it has a large potential to do so if appropriately mandated and resourced. As presented above in section 6.1, there is consensus across all categories of stakeholders for a reformed Agency, for which the main pillars can be found in existing NIS policy/law and the key strengths emerged from the evaluation. Adding full operational capabilities to ENISA would be a welcome development for some stakeholders, while it would be seen as 'unnecessary revolution' by others, in particular the most equipped Member States.

Certification

As the table 6 shows, **baseline and option 1** would not produce effective results to achieve the objectives. National and private schemes would continue to proliferate and create fragmentation. Such a trend is expected to continue, unless Member States agree on mutual recognition of their schemes or - together with the Commission - work on the development of a voluntary European scheme. However, this will occur on an ad hoc basis. In addition, as Member States would continue to use and improve their national schemes; they would also create a strong legacy, therefore making harmonisation more difficult.

End-users making cross-border purchases will not necessary understand or have access to the information regarding the security properties of the devices they have purchased. Business segments already subject to certification requirements will continue to bear costs related to multiple processes. Conversely, businesses that are currently not subject to certification requirements will not bear any upfront costs and remain free to choose whether or not to be involved in any certification process. Costs for them may arise in the future as requirements for ICT certification would be progressively put in place. No substantial upfront costs are envisaged for Member States.

These options would also yield unsatisfactory results in terms of increasing the level of assurance of critical infrastructures. The coherence with policies related to the Digital Single Market, the internal market and the NIS Directive are not fully supported, while international trade is promoted to the extent that actors concerned commit to use international standards. However, these options are expected to have positive impact on innovation and competitiveness at least in the short term. Finally, these options enjoy some support from industry, especially large, international corporations while Member States see the risk that providers of essential services operating cross-border could be subject to different security requirements in relation to ICT certification.

Option 2 would produce some effective results to achieve the objectives. The extension of the membership of the current SOG-IS MRA to all Member States provides an institutional framework that ensures mutual recognition. However, such a positive effect is expected to be limited to certification at high level of assurance. National and private schemes would continue to proliferate for a wide range of commercial products and services, thus increasing fragmentation. In addition, end-users of these products may not have the necessary information on the cybersecurity properties of these products and services. This option would produce efficient results for industry already applying for SOG-IS certificates; businesses that are currently not subject to certification requirements for their commercial products and services will not bear any upfront costs and remain free to choose whether or not to be involved in any certification process. As for efficiency, costs for Member States would vary depending on the status that thet would achieve in the SOG-IS MRA (certificate consumer or producer). Existing members of SOG-IS MRA may face an increase in demand for certification, which may translate in higher costs to accommodate such a demand but also higher revenues. This option would also produce satisfactory effects regarding the increase of the level of assurance of critical infrastructures as well as the coherence with other policies such as NIS Directive. To the extent that it ensures mutual recognition for certification of high level of assurance and it continues to utilise international standards such as CC, this option provides some support to the internal market and international trade. Finally, industry representatives as well as existing members of SOG-IS MRA agree on the need to shape future certification initiatives in Europe building on the experience of the SOG-IS MRA, but they also stress the need to significantly reform such a EU-wide mechanism.

Option 3 achieves the objectives **effectively**. This option builds on the Option 2 (e.g. extension of the existing SOG-IS MRA) but it goes much further as it envisages the creation of an institutional, voluntary framework that would allow the Commission to adopt schemes for ICT security certification, prepared by ENISA in cooperation with national authorities - represented in a dedicate Group - at various levels of assurance, thus potentially covering a wide range of products and service as the need arise. In other words, the proposed framework differs from SOG-IS MRA as the latter is one scheme while the framework is a "system" of many schemes for different product categories, different assurance levels[131] using different evaluation methods. Moreover, as it emerged from consultations and technical studies underpinning this Impact Assessment, SOG-IS MRA (a scheme built on specific CC standards) does not cover or does not respond well to market needs for a faster and cheaper certification at lower assurance levels.

In addition, Option 3 would help promote information on the cybersecurity of ICT products and services. This would be in line with the results of a Eurobarometer survey in which the majority of respondents consider that security and privacy features of an ICT product play a role in their choice. As for its **efficiency**, this Option would not imply additional, upfront costs for the industry (incl. SMEs). Rather, it would generate significant savings for those firms that already certify their products (or that are willing to carry out security certification), with beneficial effects on their competitiveness worldwide.

On the other side, it would involve some budgetary commitment to ensure the full operation of the framework at Commission, but mostly at ENISA level. Member States will have to bear the necessary costs to ensure the implementation and supervision of the framework at national level.

This option is expected to significantly support internal market by significantly reducing fragmentation. Positive impacts are also expected on international trade to the extent that the Framework backs international standards.

[131] The expression 'assurance level' should not be confused with CC EAL

Table 5 Overall impact of the various policy options for ENISA.

Impacts	Option 0: Baseline – Keep Status Quo	Option 1: Expiry of ENISA Mandate (Terminating ENISA)	Option 2 'Reformed ENISA'	Option 3: EU cybersecurity agency with full operational capabilties
Effectiveness	✖	✖✖	✓✓	✓✓✓
Economic/Efficiency	✖ (economy) ✓ (EU budget)	✖✖ (economy) ✓ (EU budget)	✓ ✓ (economy) ✖ (EU budget)	✓✓✓ (economy) ✖✖ (EU budget)
Environmental	**0**	**0**	**0**	**0**
Social	**0**	✖✖	✓✓	✓✓
Coherence	✖	✖✖✖	✓✓✓	✓✓✓
Stakeholders' support	✖	✖✖✖	✓✓ (industry) ✓✓✓ (Member States)	✓ (industry) ✓(Member States)
Total	✖✖✖	✖✖✖✖✖✖✖✖✖✖✖	✓✓✓✓✓✓✓✓✓✓✓✓	✓✓✓✓✓✓✓✓✓✓✓

The symbols "✓" and "✖" indicate respectively positive (✓) and negative (✖) impacts. For each symbol a maximum a scale 1 to 3 (maximum positive or negative assessment) is used.

Table 6 Overall impact of the various policy options for certification.

Impacts	Baseline Option 0	Option 1: Soft law measures	Option 2: extension of SOG-IS agreement to all MS	Option 3: European ICT security certification framework
Effectiveness	✖	✖	✓	✓
Economic/efficiency	**0**	✓	✓	✓✓
Environmental	**0**	**0**	**0**	**0**
Social	**0**	**0**	✓	✓
Coherence	**0**	**0**	✓	✓
Stakeholders' support	**0**	✖ (Member States) ✓ (industry)	✓ (Member States) ✓ (industry)	✓ (Member States) ✓ (industry)
Total	✖	**0**	✓✓✓✓ ✓✓	✓✓✓✓ ✓✓✓

The symbols "✓" and "✖" indicate respectively positive (✓) and negative (✖) impacts, the number of the symbols is the net result of the summing-up of the respective individual ratings of the policy option as indicated in **Annex 13** and indicates the magnitude of the change.

8. PREFERRED OPTION

Based on the above comparison, it appears that a combination of **Option 2** with regard to **ENISA** and **Option 3** for **certification** is the best option to achieve the objectives, while taking into account the criteria of efficiency and coherence.

Under this scenario, the EU would have a reformed agency for cybersecurity, focused on providing support to Member States, EU institutions and businesses in areas where it would bring the most added value: i.e. policy development and implementation; information knowledge and awareness; research; operational cooperation and crisis; market. Moreover, ENISA would play a paramount role in the field of EU cybersecurity certification policy, as it will prepare (in cooperation with MS certification authorities) candidate European cybersecurity certification schemes. The reformed ENISA would also see addressed its current weaknesses in the new mandate.

Under Option 3 for certification, the legislative proposal would provide the EU with a much needed framework of rules for establishing European cybersecurity certificates valid and recognised in 28 Member States. The framework will put the right conditions in place for effectively addressing the problem related to the co-existence of multiple certification procedures in various Member States, reducing certification costs and thus making certification in the EU overall more attractive from a commercial and competitive perspective. Altogether, this should facilitate and improve (in the short-medium run) businesses' cyber-certification practices, thereby contributing to the spreading of better cybersecurity practices in the design of ICT products and services (security by design).

The solution to combine these options is therefore considered the most effective for the EU to reach the identified objectives of: increasing cybersecurity capabilities, preparedness, cooperation, awareness, transparency and avoiding market fragmentation.

This combination of options is also the most coherent with policy priorities, as it is entrenched in the Cybersecurity Strategy and related policies (e.g. NIS Directive), and the Digital Single Market Strategy. In addition, from the consultations carried out so far, it clearly emerges that the preferred options enjoy the favour of the majority of stakeholders.

Furthermore, the analysis conducted in this impact assessment demonstrates that the combination of these two options would reach the objectives through a reasonable employment of resources. In particular, a 'reformed ENISA' would provide Member States with a more adequate support to achieve cyber resilience, and will only have a limited impact on the EU budget. At the same time, a voluntary European certification framework will help promote the cybersecurity of digital products and services in the EU, with a limited impact on the resources of Member States and EU budget, and no upfront costs for industry.

In line with the principle of proportionality, the preferred option proposes actions that are not considered going beyond what is necessary to achieve the objectives defined in this impact assessment. In addition, the nature of the objectives is such that they cannot be achieved sufficiently by a unilateral action of Member States. For this purpose, an intervention at Union level is necessary.

Finally, linking the review of the ENISA mandate with the measures on certification is a coherent way to address the common problem mainly related to insufficient cyber awareness, and the fragmentation of policies and approaches towards cybersecurity across Member States. As explained throughout the document, security certification is an area in which such a fragmentation is increasingly emerging and greater awareness is

particularly needed. This creates a negative impact on the internal market. As an internal market agency, and as further confirmed in the evaluation process and the stakeholders consultations, ENISA is best placed to support a coherent approach to security certification across the EU.

The establishment of a European legal framework would be a first step to develop a common policy in this field, build consensus on new priority areas to tackle and plan future activities, as needs arise. In a fast-moving, dynamic market, such as the one of ICT products and services, this approach would create the conditions for key decisions to be taken in the future by the competent authorities, such as the matching between the products/services and the needed level of security.

The preferred option entails EU legislative intervention as only a binding instrument can guarantee the translation into practice of the measures proposed and the achievement of the related specific objectives. The chosen legal instrument is a Regulation that will cover the new mandate for ENISA and lay down a European ICT security certification framework.

Table 7 Overview of main changes in the tasks between current ENISA and preferred option

Areas	Before	Factors of change	After
Policy development and implementation	• Assisting and advising on all matters relating to Union NIS policy and law • preparatory work, advice and analyses relating to the development and update of Union NIS policy and law • Analyzing publicly available NIS strategies and promoting their publication	• Strengthen/refocus existing mandate • New tasks/align to subsequent legislation (e.g. NIS Directive , eIDAS, Electronic Communications Code)	• Actively contribute its independent opinion to policy development and implementation in the area of cybersecurity including in sectoral law and policy where cybersecurity is involved • contribute to the work of the Cooperation Group, pursuant to Article 11 of NIS Directive, by providing its expertise and assistance • supporting the development and implementation of Union policy in the area of electronic identity and trust services (eIDAS) • supporting the promotion of an enhanced level of security of electronic communications (Code) • supporting regular

			review of the EU cybersecurity policy and law (annual report including summary notifications as per NIS Directive, eIDAS and Code)
Capacity building	• supporting MSs at their request, to develop and improve the prevention, detection and analysis of and the capability to respond to NIS problems and incidents • assisting the EU institutions, bodies, offices and agencies in their efforts to develop the prevention, detection and analysis of and the capability to respond to NIS problems and incidents, in particular by supporting the operation of a CERT for them. • Offering NIS training for relevant public bodies, • supporting the raising of the level of capabilities of national/governmental and Union CERTs, including by promoting dialogue and exchange of information, with a view to ensuring that, with regard to the state of the art, each CERT meets a common set of minimum capabilities and operates according to best practices	• Strengthen/refocus existing mandate • Align to NIS Directive • New tasks	• Keep mandate with regard to trainings, CSIRTs maturity and general principle of assistance to Member States and EU institutions • support the development and review of EU cybersecurity strategies, promoting their dissemination and tracking progress of their implementation • assist Member States in developing national NIS strategies pursuant to Article 7(2) of Directive (EU) 2016/1148 • assist Member States, upon their request, in developing national CSIRTs pursuant to Article 9(5) of NIS Directive • assist the Cooperation Group, with exchanging of best practices, in particular with regard to the identification of operators of essential services, including in relation to cross-border dependencies, regarding risks and incidents, pursuant to Article 11(3)(l) of NIS Directive
Market	Facilitating the	• Strengthen/refocus	1)Standardization: keep

	establishment and take-up of European and international standards for risk management	existing mandate • Align with NIS Directive • New tasks	mandate and align with Article 19 (2) of NIS Directive with regard to collaboration with Member States to draw up advice and guidelines regarding the technical areas to be considered. 2) Certification: support Union policy development and implementation; contribute to development and maintenance of the ICT security certification framework. 3) Market Observatory: analyses and dissemination of the main trends in the cybersecurity market.
Operational cooperation	• Promoting dialogue and exchange of information between national/governmental CERTs, including CERT-EU • Provide advice to EU institutions and Member States, upon request, in the event of breach of security or loss of integrity with a significant impact on the operation of networks and services • Organizing Cybersecurity exercises • supporting the development of a Union early warning mechanism that is complementary to MSs' mechanisms • promoting and facilitating voluntary cooperation among Member States and between EU institutions and the Member States in their efforts to prevent, detect and	• Strengthen/refocus existing mandate • New tasks • Align to subsequent legislation (NIS Directive) and the new initiatives (Blueprint)	• Establishing systematic cooperation on operational matters with EU institutions, agencies and bodies, in particular CERT-EU and EC3 • Providing the secretariat of the CSIRTs network as per NIS Directive and actively facilitating the information sharing and the cooperation. • Contribute to operational cooperation within the CSIRT Network, providing, in cooperation with CERT-EU, support to Member States that would request it by: 1. Advising on how to improve their capabilities to prevent, detect and respond to incidents. 2. Providing technical

	respond to cross-border incidents		assistance in case of significant cybersecurity incident. 3. Ensuring backend support for analysis of vulnerabilities, artefacts and incidents in order to strengthen preventive and response capabilities of Member States • Organizing Cybersecurity exercises • Contribute to the blueprint, supporting a cooperative EU response to large scale cross-border cybersecurity incidents and crises, mainly by: 1. Aggregating reports from national sources with a view to establish common situation awareness; 2. Ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRT Network and the technical and political decision makers; 3. Supporting technical handling of the incident, including facilitating sharing of technical solutions between Member States; 4. Supporting the handling of the Union public communication around the incident;

			5. Testing the Union cooperation plans to respond to cross-border incidents and crises
Research and Innovation	Advising the Union and the Member States on research needs in the NIS area	• Strengthen/refocus existing mandate • New task	• Advice on research needs and priorities and feed into the Hub of Excellence • Upon request of Commission participate in implementation of R&I Programmes
Knowledge, information, awareness	• assisting the Union institutions, bodies, offices and agencies and the MSs in their efforts to collect, analyse and, in line with MSs' security requirements, disseminate relevant NIS data • providing Member States with the necessary knowledge to improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents. • promoting the development and sharing of best practices • promoting best practices in information sharing and awareness raising • supporting the EU and the Member States in organizing awareness raising	• Strengthen/refocus existing mandate • New Tasks	• Analyses of emerging technologies and assessment of economic, societal, legal, regulatory impacts on cybersecurity • Advice, guidance and best practices, in cooperation with Member States experts, for the security of NIS, in particular internet infrastructures and those related to sectors listed in NIS Directive • Information Hub: one-stop-shop for information on cybersecurity deriving from EU institutions, agencies and bodies. • Compile reports based on public information after cyber incidents to provide guidance to citizens and businesses • Raise awareness about cyber hygiene good practices • Keep mandate on awareness raising campaigns (e.g. Cybersecurity

			Month)

Case studies on the preferred option:

An example of Reformed ENISA in the event of a cyber crisis

Box 5 – Before/after (fictional) scenario of large scale cross-border cyber incident

1. "Before" scenario

A new computer virus infects the systems of the national branch office of a major accounting firm. Citizens and companies are not sufficiently aware of cyber threats and do not have sufficient information of cyber hygiene practices, so the virus spreads with phishing emails to clients across the EU. National experts scramble to determine how the virus works and how to stop its spread, information is shared only between a few members within the CSIRT Network and ENISA does not have the capacity to monitor the situation and provide assistance to those Member States who do not have sufficient resources. There is no rehearsed coordination plan between ENISA, CERT-EU and EC3 and between Member States and the EU bodies. The lack of a common EU situation awareness slows down the identification of the root causes and the estimation of the scale of the event. The computer virus continues to spread rapidly across the EU and the affected companies take their IT systems off-line to contain the damage. Incident responders are overwhelmed by the increasing number of incidents at national level and there is no assistance available at EU level to help technical handling of the incidents. In the aftermath of the event, some countries do not have the necessary resources to conduct incident analysis. Some Member States authorities publish reports and recommendations, in national language, for the future targeting businesses and citizens.

2. "After" scenario

A new virus infects systems of the national branch office of a major accounting firm. Citizens' and companies are better informed of cyber threats and how to address them: ENISA, in cooperation with experts from Member States, regularly provides guidance and best practices, for the security of network information systems and it provides cyber hygiene recommendations targeted. As a consequence, the spread of the virus is somehow contained in comparison to scenario 1 as more users are able to detect phishing emails. However, some Member States are still severely affected. The CSIRT Network swiftly goes into information sharing mode, ENISA runs efficiently the communication channels and ensures that the competent actors at EU level are kept informed so to allow swift decision making. Operational cooperation and coordinated activities allow for faster identification of the causes of the incident. The spread of the computer virus continues to slow across the EU. The infected companies across the EU have at hand good practices and guidance about how to deal with incidents and are able to maintain key services running. ENISA and CERT-EU experts provide assistance to national incident responders that request help with mitigating measures, based on the solution adopted in other Member States. They are also assisted with restoring IT services and incident analysis. Based on a thorough analysis of the incident and the information made available at Member State level, ENISA compiles an EU wide report on the event with recommendations for future.

Examples of how the EU Cybersecurity Certification Framework would change the present situation.

1. Smart meters

	Now	Future
Requirements	• In order to sell in UK and France manufacturers have to certify against different schemes: o CPA (Commercial Product Assurance) in UK, o CSPN (Certification de Sécurité de Premier Niveau) in France	• Manufacturers will need to undergo a single certification process, as envisaged in the future European certification scheme for smart meters. The resulting certificate will be accepted by all public authorities in Member States.
Cost	• The overall cost is at least 300 thousand euros for the two markets (about 150 thousand euro in UK and about 150 thousand euros in France).	• The estimation of costs saving ranges up **to 80% of current costs**
Time	• **6 to 18 months.** This estimate takes into account: o Completion of multiple certifications processes and supporting documentation o Identification of various requirements that a vendors needs to comply with. o limited number of conformity assessment bodies able to certify against the requirements of different schemes.	• **Faster process** that takes into account: o Role of ENISA that provides information needed for compliance with the European scheme (e.g. specialised conformity assessment; documentation) o Completion of single process : no multiple certifications are needed and capacities of existing CABs can be used more efficiently
Other	• **Different methodologies** for risk assessment and definition of security requirements	• **Standard methodologies** for risk assessment and definition of security requirements

2. Cloud Computing

	Now	Future
Requirements	• In order to sell Cloud Computing Products / Services in France and Germany providers have to certify against:SecNumCloud **and** Compliance Controls Catalogue (C5)	• Providers need to undergo a single certification process, as envisaged in the future European certification scheme for cloud computing. The resulting certificate will be accepted by all public authorities in Member States
Cost	• Costs associated to compliance with different technical rules and multiple testing is estimated around 1.2 billion euro, that accounts for **2% to 10%** of companies' annual expenditures.	• An increased level of competition, introducing an EU wide Certification Scheme, would result in a **yearly saving of € 1.1 billion in the EU public sector alone**
Time	• **Around 7-9 months** due to the multiple audit and testing processes to obtain several certifications	• **Reduced time**: duration of a single process is estimated to take around 4 to 6 months. ENISA would accelerate the process by providing the information needed for compliance with the European scheme
Other	• Faced with co-existence of multiple schemes and standards[132], end-users (esp. in the banking sector) are not able to compare and judge which scheme or standard would best satisfy their particular security requirements. This deteriorates the trust in cloud computing services.	• The existence of a security certification scheme for cloud computing agreed at EU level, increases the trust in this service • Competitive gain for cloud providers due to cost and time reduction

9. HOW WILL ACTUAL IMPACTS BE MONITORED AND EVALUATED?

This section describes the monitoring and evaluation that could be applied to assess the impact of the objectives and the preferred option.

Monitoring will start right after the adoption of the legal instrument and it will focus on its application. The Commission will organise meetings with ENISA, Member States representatives (e.g. group of experts) and the relevant stakeholders in particular to

[132] ECSO has published a State-of-the-Art Syllabus listing 6 different schemes and 2 standards to certify the security of cloud computing services.

facilitate the implementation of the rules concerning certification such as the establishment of the Cybersecurity Certification Group.

In particular, monitoring activities on certification will consider the widening of the product and services scope covered by EU certification schemes. This would help better evaluate the potential uptake and interest in the setting up of EU-level certification schemes. Moreover, an eventual decrease of national initiatives or industry-driven schemes would equally provide an indication of a reduced level of fragmentation in the certification landscape in the EU. Similarly, it would signal a positive move towards a proper functioning of the EU internal market for ICT products and services. Transparency elements such as publication of cybersecurity market trends in Europe and surveying the awareness of security features of ICT products and services among end-users and businesses would provide further indications.

The first evaluation should take place five years after the entry into force of the legal instrument, provided sufficient data is available. An explicit evalaution and review clause, by which the Commission will conduct an independent evalaution, will be included in the legal instrument. The Commission will subsequently report to the European Parliament and the Council on its evaluation accompanied where appropriate by a proposal for its review, in order to measure the impact of the Regulation and its added value. Further evaluations should take place every five years. The Commission Better Regulation methodology on evaluation will be applied. These evaluations will be conducted with the help of targeted, expert discussions, studies and wide stakeholders consultations.

ENISA's Executive Director should present to the Management Board an ex-post evaluation of ENISA's activities every two years. The Agency should also prepare a follow-up action plan regarding the conclusions of retrospective evaluations and report on progress bi-annually to the Commission. The Management Board should be responsible to vigilate on the adequate follow-up of such conclusions.

Alleged instances of maladministration in the activities of the Agency may be subject to inquiries by the European Ombudsman in accordance with the provisions of Article 228 of the Treaty.

The list of monitoring indicators that could be used to monitor progress towards meeting the general and specific objectives is presented in table 8 below. The data sources for planned monitoring would mostly be ENISA, the European Cyber-Certification Group, the Cooperation Group, the CSIRT Network and the Member States' authorities. Besides the data deriving by the reports (including the annual activity reports) of ENISA, the European Cyber-Certification Group, the Cooperation Group and the CSIRTs Network, specific data gathering tools will be used when needed (for example surveys to national authorities, Eurobarometer and reports from Cybersecurity Month campaign and the pan-European exercises).

Table 8 List of indicators to monitor progress towards general objectives

General Objectives	Specific Objectives	Operational objectives	Monitoring indicators	Source of data
Increase the cyber resilience of the Member States, businesses and the EU as a whole.	Increasing **capabilities and preparedness** of Member States and businesses, in particular the critical infrastructures	• To contribute effectively to the development of policy in the area of NIS as well as policy initiatives with cybersecurity elements in key sector (e.g. Energy, Transport, Finance, etc). • To support the development and necessary updates to National and EU Cybersecurity Strategies. • To contribute to improvement of national public authorities' capabilities expertise, in particular in cybersecurity incident response (CSIRTs) and supervision of cybersecurity related regulatory measures. • To provide Member States and businesses with long-term strategic analyses of cyber threats, incidents to identify emerging trends. • To facilitate the establishment and take-up of European and	• Number of trainings organised by ENISA • Geographical coverage (number of countries and areas) of the direct assistance provided by ENISA • Level of preparedness reached by Member States in terms of CSIRT maturity and supervision of cybersecurity related regulatory measures • Number of EU-wide good practices for critical infrastructures provided by ENISA • Number of EU-wide good practices for SMEs provided by ENISA • Publication of annual strategic analysis of cyber threats and incidents to identify emerging trends by ENISA • Regular contribution of ENISA to the work of cybersecurity working groups of the European Standardisation	ENISA ENISA CSIRT Network and ENISA ENISA ENISA ENISA ENISA European Cybersecurity Certification Group (ECCG)

		international standards for risk management and for the security of electronic products, networks and services	Organisations (ESOs). • Number of conformity assessment bodies specialized in ICT certification, across Member States	
	Improving **cooperation and coordination** across Member States and EU, institutions, agencies and bodies	• To ensure the coherence and the adequacy of the EU regulatory approach to cybersecurity • To contribute to the evaluation and review of cybersecurity related policies in the EU. • To establishing information exchange networks between administrations, industry and end user representatives in the NIS community • To contribute to the establishment of Information Sharing and Analysis Centres in various sectors. • To pool, organize and make available information on cybersecurity deriving from the EU institutions, agencies and bodies. • To provide	• Number of Member States having made use of ENISA recommendations and opinions in their policy making process • Number of EU institutions, agencies and bodies having made use of ENISA recommendations and opinions in their policy making process • Regular implementation of CSIRT Network work programme and well-functioning on the CSIRTs Network IT infrastructure and communication channels • Number of technical reports made available to and used by the Cooperation Group • Consistent approach to the NIS Directive implementation across borders and sectors • Number of regulatory compliance assessments performed by ENISA	Survey of Member States authorities (study) Survey of EU institutions, agencies and bodies (study) ENISA and CSIRT Network ENISA ENISA ENISA and ECCG ENISA

		recommendations to Member States and the Commission on priority-setting in research and developments. • To achieve a structural cooperation with CERT-EU and EC3, in particular on operational matters.	• Number of ISACS in place in different sectors, in particular for critical infrastructures • Establishment and regular running of information platform disseminating cybersecurity information deriving from the EU institutions, agencies and bodies • Regular contribution to the preparation of EU research and innovation work programmes • Cooperation agreement between ENISA, EC3 and CERT-EU in place • Number of certification schemes included and developed under the Framework	Commission Commission ENISA ECCG
	Increasing **EU level capabilities to complement the action of Member States**, in particular in the case of cross-border cyber crises.	• To assist Member States in proactively identifying cybersecurity risks and vulnerabilities and monitoring and reporting incidents • To Assist Member States in establishing appropriate response mechanisms	• Publication of annual strategic analysis of cyber threats and incidents to identify emerging trends by ENISA • Publication of aggregated information of incident reported under NIS Directive by ENISA	ENISA ENISA

		• To support a cooperative EU response to large scale cross-border cybersecurity incidents and crises	• Number of pan-European exercises coordinated by the Agency and number of Member States and organisations involved. • Number of requests to support emergency response by Member States to ENISA and performed by the Agency • Number of analyses of vulnerabilities, artefacts and incidents performed by ENISA in cooperation with CERT-EU. • Availability of EU-wide situational reports based on information made available to ENISA by Member States and other entities in case of large scale cross-border cyber incident.	ENISA ENISA ENISA and CERT-EU ENISA
	Increasing **awareness** of citizens and businesses of cybersecurity issues.	• To raise awareness of citizens and businesses of cybersecurity threats and cyber hygiene practices. • To promote and share cybersecurity best practices from across the EU	• Regular running of EU-wide and national awareness raising campaigns and regular update of the topics according to the emerging learning needs. • Increase of cyber awareness among EU citizens • Regular running of	ENISA Eurobarometer ENISA

			cybersecurity awareness quiz and increase over the time of the percentage of correct responses. • Regular publication of cybersecurity and cyber hygiene good practices targeted to employees and organisations.	ENISA
Ensure the **proper functioning of the EU internal market** for ICT products and services.	Avoiding **fragmentation of certification schemes** in the EU and related security requirements and evaluation criteria across MS and sectors.	• To develop an EU ICT Security Certification Framework based on mutual recognition of certification schemes • To support ICT security certification policy development and implementation	• Number of schemes that adhere to the EU framework • Guidelines for certification according to the EU framework in place • Set-up of the European Cybersecurity Certification Group and regular organisation of meetings • Reduced cost of obtaining a certificate for ICT security.	ECCG, ENISA ECCG, ENISA ENISA Survey of EU companies (study)
		• To support alignment of alignment of the demand and supply of cybersecurity market in the EU	• Regular publication of analyses of the main trends in the EU cybersecurity market	ENISA
	Increasing the overall **transparency of cybersecurity assurance** of ICT products and services so as to strengthen trust in the digital single market	• To widen the scope of the products that are certified • To ensure better information for the buyers of the	• Number of certified ICT products and services according to the rules of the European ICT security certification framework	ENISA

	and in digital innovation	security features of ICT products and services	• Increase in the number of end-users who are aware of security features of ICT products and services	Eurobarometer and survey of EU companies (study)
Increase the global competitiveness of the EU companies operating in the ICT field.		• To avoid that EU companies lose competitiveness due to the need to undergo several certification procedures	• Number of schemes that adhere to the EU framework.	ENISA

Annex 1: Procedural information

10. LEAD DG, DECIDE PLANNING / CWP REFERENCES

This Impact Assessment Report was prepared by Directorate H "Digital Society, Trust and Cybersecurity" of the Directorate General "Communications Networks, Content and Technology" (DG CNECT).

The Decide Planning reference of the initiative "Proposal for a Regulation of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA), repealing Regulation (EU) No. 526/2013 and laying down a European security certification framework for Information and Communications Technology (ICT) Products and Services" is 2017/CNECT/005.

The initiative on the review of ENISA was included in the Commission Work Programme for 2017.

11. ORGANISATION AND TIMING

Several services of the Commission with an 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. In 2017, this group was further enlarged to discuss the review of the initiative involving the review of ENISA Regulation and the European ICT security certification framework.

In 2016, two meetings of the ISG on the review of ENISA were held. The first meeting took place on 24 June 2016. DG CNECT, DG HOME, JRC, DG JUST, the Secretariat General (SG) and EEAS participated in the meeting. The second meeting was held on 9 December, 2016. The representatives from DG CNECT, DG DIGIT, SG and EEAS were present.

The third ISG meeting was dedicated to the review of ENISA and the set-up of a European ICT security certification framework, and took place on 24 May, 2017. The meeting was chaired by SG, and DG CNECT was flanked by DG BUDG, DG COMP, DG DGIT, DG EMPL, DG ENER, DG FISMA, DG GROW, DG HOME, DG HR, DG NEAR, DG TRADE, and EEAS.

The fourth ISG meeting took place on 22 June, 2017. This was the last meeting of the ISG before the submission to the Regulatory Scrutiny Board (RSB) on 28 June, 2017.. The meeting was chaired by SG and the participants were the following: DG BUDG, DG DGIT, DG EMPL, DG ENER, DG GROW, DG HOME, DG HR, DG JUST, the Legal Service (LS), DG MOVE, DG TAXUD, and DG TRADE. DG CNECT has updated the Impact Assessment Report by taking into account the comments received at - and following - the ISG meeting, in particular the comments made by, DG GROW, DG JUST, LS, DG TRADE, and SG. Following a positive opinion issued by the RSB, a final Fast Track ISG meeting was held on 30 August

12. EXCEPTIONS TO THE BETTER REGULATION GUIDELINES

DG CNECT has identified one exception to the Better Regulation Guidelines. Specifically, a dedicated public consultation focussing on ICT security certification in the EU has not been conducted. However, stakeholders were given the opportunity to express their views on the issue of ICT security certification in the following public consultations:

- The public consultation on the public-private partnership on cybersecurity and possible accompanying measures that took place in 2016; and
- The public consultation on the review and evaluation of ENISA, conducted in 2017.

Additionally, two surveys regarding ICT security certification have been organised in 2017 to complement the results of the past consultations:

- The survey on ICT security certification, targeting the certification community and organised by ENISA; and
- The small and medium enterprises survey on ICT certification and security framework was closed on 30 June, 2017 and final results were used in the revised report. The survey is currently also being broadened and results may be available in September.

13. CONSULTATION OF THE REGULATORY SCRUTINY BOARD (RSB)

The Impact Assessment report was examined by the Regulatory Scrutiny Board on 19 July, 2017. On 25 August the Board issued a draft positive opinion with reservations. The table below summarises how the comments of the Board and of other Services have been addressed.

Board's Recommendations in the Opinion	Implementation of the recommendations

of 25 August 2017	into the revised IA Report
The report does not describe the EU cybersecurity context well, e.g. the blueprint on large scale cross-border incidents. In addition, some ambiguity remains concerning the current application of mutual recognition (e.g. why it does not apply by default to ICT products) and the resulting limits to free movement of goods and reported market fragmentation	The report has been updated, in particular with regard to the glossary, the section 1 (context), section 5.1 (baseline scenario) and the section 5.3 (options related to certification). The meaning of cybersecurity for the purpose of the analysis and how it interrelates with network and information systems and their security. More details on the EU cybersecurity context, in particular the measures that are included in the Communication on Cybersecurity (September 2017[133]) and have a special relevance for ENISA: the EU cybersecurity blueprint, where the Agency is expected to play a major role in supporting the development of a cooperative approach to respond to large scale cross-border incidents; and the European Cybersecurity Research and Competence Centre, to which the Agency would link its advisories on EU research needs. It is also clarified that the policy options for

[133] JOIN(2017) 450

	certification refer to shortcomings related to the mutual recognition of certificates resulting from national certification schemes and not of products themselves. Such a mutual recognition may occur in an uncoordinated manner and would depend on the willingness of each Member States. It is further specified that, in absence of mandatory requirements for certification, uncertified products and services can still circulate. Requirements for certification are not necessary mandatory but can be market-driven. In the latter case, customers are presumably more willing to purchase certified products, as they assign a high value to the information provided by certification.
The report ignores the evaluation findings on ENISA weaknesses. It overlooks risks associated with ENISA's ability to absorb additional resources and to deliver effectively on an enlarged mandate.	The report has been further integrated to provide clarifications on the new obligations in the policy options related to ENISA (section 5.2) and on how some weaknesses related to ENISA efficiency, highlighted in the evaluation, are expected to be addressed (section 6.1. assessment of the impact). In particular explanations are provided on how the reform of the Agency, including the new tasks, the better conditions of employment and the structural cooperation with CERT-EU, would improve its attractiveness as employer and help tackle problems related to

	the recruitment of experts. Annex 6 to the report also presents a revised estimate of costs (for ENISA) associated to policy options 2 and 3.
The preferred option regarding certification is unclear. The report does not spell out how certification would work in practice. This makes it hard to assess potential value added, feasibility and cost. There is a risk that ENISA would not deliver much on certification.	Section 5.3 (description of the preferred policy option on certification) and 6.2 (assessment of the impact of policy options) have been revised in order to provide a more detailed explanation of option 3, including a graphic. The section on impact of option 3 also includes estimates on the costs for Member States, associated with supervising and enforcement activities as well as on the staff and resource implications for the Commission related to the new certification framework (e.g. set up of Expert Group). In addition, section 7 on option comparison and 6.2 on impact of option 3 (section on efficiency), includes an explanation of how the proposed framework differs and improves the current SOG-IS system. The rationale for the choice of ENISA as expert in the field and the only EU level agency on cybersecurity has been detailed in section 6.2
The range of products to which certification could apply remains unclear and so do the	The revised description of Option 3 explains that the type of ICT product and service

resulting impact	covered by a European certification scheme will be defined in the approved scheme itself.
What are the risks and consequences of Member States not adopting or using EU schemes?	The section on the impact of option 3, (objective 2) for certification specifies that Member States not using European certification schemes may face pressure from other Member States using these schemes to protect their assets
While the report provides additional information of costs, it does not sufficiently describe the magnitude of expected tangible benefits and how they compare across options	The sections on the impact of option 1 and 2 have been revised to better describe the benefits of these options. In particular Option 1 would help deliver the policy objectives faster and in a more cost-effective manner. Option 2 would provide Member States with institutional fora, enabling all Member States to express their security needs. Option 2 would also lead to a strengthened European position in the international context, and may become a model for other world's region.
The monitoring and evaluation framework lacks criteria and benchmarks for measuring success.	Section 9 of the report had been previously updated to address the comment of the Board according to which the table for M&E was useful and detailed but it lacked information on the origin and frequency of data collection. Further elements to evaluate the positive impact of the initiative on certification (e.g. monitoring of decrease of fragmentation and uptake of EU-level

	schemes) have been added
Presentation	Newly introduced abbreviations (e.g. IPCR and ARGUS) have been added to the glossary

14. EVIDENCE, SOURCES AND QUALITY

The Commission gathered qualitative and quantitative evidence from various sources:

(1) Two public consultations (a summary of which is attached to Annex 2 to this report) regarding:
   a. The evaluation and review of ENISA; and
   b. The public-private partnership on cybersecurity and possible accompanying measures (included a Section on ICT security certification).
(2) Four stakeholder workshops with Member States and industry:
   a. Three regarding ICT security certification; and
   b. One regarding the ENISA review.
(3) Fifty expert interviews regarding the ENISA review.
(4) A survey on the ENISA review to the Computer Security Incident Response Teams Network.
(5) A survey to the ENISA Management Board, Executive Board, Permanent Stakeholder Group, and ENISA staff.
(6) Three technical studies:
   a. One final draft report on the evaluation and review of ENISA prepared by an external contractor; and
   b. Two studies regarding ICT security certification (one conducted by the Joint Research Centre (JRC), and another one by an external contractor).
(7) A survey on certification and labelling addressed to small and medium enterprises (SMEs).
(8) A survey for national cybersecurity authorities, industry and consumer associations on certification and labelling conducted by ENISA;

(9) Inputs regarding ICT security certification from the European Cybersecurity Organisation (ECSO);
(10) Direct dialogue with stakeholders, in particular through ad hoc meetings with representatives of interested industries, in particular regarding ICT security certification.
(11) A roundtable with European Commission Vice-President for the Digital Single Market, Andrus Ansip, on 25 April 2017.
(12) Desk research and literature review done in-house by DG CONNECT.

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

- The survey on certification and labelling addressed to SMEs closed on 30 June 2017;
- The ENISA study is a final draft report;
- There are limitations with regard to gathering data. For instance, the public consultation on the ENISA review received 90 submissions, and CNECT has not received much input from SMEs in our input-gathering exercise. 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;
- The quality of the studies is impacted by the overall lack of evidence in the field of cybersecurity as a whole. In particular, companies are reluctant to share information regarding cybersecurity, considering that reporting on these topics could potentially harm them. In addition, there is no overall agreed taxonomy. This is one of the issues that the initiative is aiming to tackle.
- As regards to the survey on ENISA that was addressed to CERTs and CSIRTs, and the survey on the European ICT security certification framework addressed to SMEs, 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 this, and might then have reopened it using a different browser or device to complete the survey then. This would result in a double counting of the answers.

Annex 2: Stakeholder Consultation

15. Stakeholder Consultation Strategy

In order to make sure that the Union's general public interest – as opposed to special interests of a narrow range of stakeholder groups – is well reflected in the assessment of the initiative, the Commission developed a stakeholder strategy to ensure the widest consultation possible. This strategy ensures transparency and accountability in the Commission's work.

In order to identify the most appropriate mix of consultation methods, the first step has been to identify the relevant stakeholder groups and the best way to consult them in order to gather relevant input.

The Commission pays attention to differentiate data gathering tools and adapts them to different types of contributions the stakeholders might have (See Section **2.2** below). Furthermore, in order to allow for wide participation, the consultation period spanned over a long period - from July 2016 to May 2017 approximately.

In view of the wide variety of sources and stakeholders consulted, and the relatively high degree of responses and input received from all stakeholders' group, the stakeholders views hereby discussed are considered as overall representative.

As regards the methodology and tools, the basic analysis approach has been largely adopted. Responses have been mostly grouped into broad stakeholder groups (e.g. Member State authorities, respondents from private sector, other respondents, etc.). Responses from a particular group on a particular issue helped provide an overview of the most recurrent points being made.

16. Identification of groups of stakeholders consulted, means of consultation, and consultation topics

16.1. Whom has the Commission consulted?

A non-exhaustive list of stakeholders that have been consulted (for both the review of ENISA and the EU ICT security certification framework, unless otherwise indicated below), includes the following bodies:

- The EU Member States national authorities as well as those from European Free Trade Association (EFTA) Countries;
- Standardisation bodies;
- Senior Officials Group – Information Systems Security (SOG-IS) members (mostly regarding certification);
- The members of ENISA's Management Board, Executive Board, Permanent Stakeholder Group and Network of Liaison Officers;
- Trade associations and industry representatives, including the European Cybersecurity Organisation (ECSO), Alliance for Internet of Things Innovation (AIOTI), DigitalEurope, and the Enterprise Europe Network (in particular for small and medium enterprises (SMEs);
- Consumers' representatives;
- Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) (mostly regarding ENISA);
- European Commission's services;
- The European External Action Service, the European Parliament, the Council of the European Union, the European Economic and Social Committee, the Committee of the Regions; the European Court of Auditors;
- Other EU Agencies and bodies, such as Computer Emergency Response Team for the EU institutions (CERT-EU), Europol and its European Cybercrime Centre (EC3), European Defence Agency, Body of European Regulators for Electronic Communications (BEREC), European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice (Eu-LISA) (mostly regarding ENISA);
- International Organisations; and
- Citizens.

16.2. How has the Commission consulted stakeholders?

Depending on the stakeholder group identified, different tools and methods were used in order to conduct the consultation.

- During a 4-week period, all interested stakeholders were able to provide feedback on the ENISA evaluation roadmap.
- Public Consultations:

- In 2016, a 12-week online public consultation was carried out at the occasion of the launch of the contractual public-private partnership on cybersecurity, which included specific questions / section on the topic of certification (approx. 240 respondents).

- In 2017, a 12-week online public consultation was carried out to seek views from the wider public (approx. 90 respondents) on ENISA evaluation and review. The consultation included also questions on the future needs and priorities in the area of cybersecurity, including the topic of certification.

- Survey targeted at ENISA staff and management, Management Board, Executive Board, Permanent Stakeholder Group, Network of Liaison Officers to cover more in-depth issues related to the efficiency and the effectiveness of the Agency and to its governance and organisation.
- Survey on ENISA targeted at the Computer Security Incident Response Teams Network (CSIRTs), for which the Agency provides the secretariat according to the NIS Directive.
- In-depth interviews, with approximatively 50 key players in the cybersecurity community on the ENISA review, including on its role in certification.
- Stakeholder workshops:

  - In 2016, 2 workshops with national authorities were held on the topic of certification;

  - In 2017, 2 workshops were carried out on the ENISA review and certification respectively.

- Survey of national certification authorities, industry, consumers associations on the topic of certification and labelling, conducted by ENISA and the Commission.
- A targeted questionnaire on the topic of ICT security certification and labelling was conducted in June 2017.
- Inputs from the European Cyber Security Organisation (ECSO) on the challenges of certification and labelling. Working Group 1 of ECSO on certification and labelling includes 236 registered experts.
- Direct dialogue with individual stakeholders reaching out to the Commission on ENISA review and certification.

17. HAVE THE COMMISSION STANDARDS BEEN MET?

The Commission standards as set in the Better Regulation Guidelines have been met. However, please see the exception to the Better Regulation Guidelines identified in Annex 1, points 3 and 5.

18. SUMMARY OF RESULTS FROM THE CONSULTATIONS REGARDING ENISA

18.1. Results of the public consultation on the evaluation and review of ENISA

The open public consultation on the evaluation and review of ENISA took place between 18 January and 12 April 2017. The public consultation aimed to gather the views of stakeholders and interested parties to assess ENISA's overall contribution to the cybersecurity landscape for the period 2013 to 2016. The public consultation also contributed to a reflection on potential policy options for the revision of ENISA's mandate. For this purpose, the consultation was structured around two sections:

- Backward looking – ex-post evaluation of ENISA; and
- Forward looking – focusing on evolving needs and challenges in the cybersecurity landscape and the possible role of an EU body to meet them in the future.

Respondents were allowed to answer either one or both sections. In addition, respondents had the possibility to send position papers.

With a total of 90 responses, the results of this 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 to cybersecurity.

Main results related to the backward looking questions:

- The overall performance of ENISA during the period 2013 to 2016 was positively assessed by a majority of respondents (74%). A majority of respondents furthermore considered ENISA to be achieving its different objectives (at least 63% for each of the objectives).

- ENISA's services and products are regularly (monthly or more often) used by almost half of the respondents (46%) and are appreciated for the fact that they stem from an EU-level body (83%) and for their quality (62%).

- A majority of respondents considered ENISA's size in terms of staff members to be insufficient (59%).

Main results related to the backward looking questions regarding specific topics:

1. Interaction with ENISA

    - Among the respondents, 50% interacted with ENISA's products and services "a few times per year" or only "on to two times per year", while 46% of respondents interacted "on a weekly basis" or "on a monthly basis".

    - When comparing the frequency of interaction with ENISA or the use of ENISA's products and services within a given group, 47% of the national authority respondents interact "on a weekly basis", while the largest proportion of private enterprise and business association respondents (50%) do so "a few times per year" and 35% of "other respondents" interact "one to two times per year".

    - National authorities most frequently indicated "Guidelines & recommendations, including on standards" as being either "relevant" or "very relevant" to their work / activities.

    - Among private enterprises or business associations, the products or services most frequently selected as being "(very) relevant" to respondents' work / activities were "Reports & Research Publications" as well as "Events". "Training material or toolkit" was most often selected as being only "somewhat" or "not relevant". The group of "other" respondents gave the same assessment for this service.

2. *ENISA's contribution to NIS in the EU*

    - All respondents to the public consultation indicated that ENISA had achieved its targeted objectives to some or to a great extent.

    - The objective of "Developing and maintaining a high level of expertise in cybersecurity" was selected as being achieved to a "great extent" or to "some extent" by the highest number of respondents (86% or 56), followed by "Supporting cooperation in the cybersecurity community, e.g. through public-private cooperation, information sharing, enhancing community building, coordinating the Cyber Europe Exercise" (79% or 51).

- When comparing the responses of different stakeholder categories, the results showed that the three categories felt different about which objectives had been met to a "great" or to "some extent".
    - All national authorities (100% or 15) indicated that "Supporting the implementation of EU policy" had been achieved "to a great extent" or "to some extent".
    - Private enterprises or business associations (71% or 17) most frequently indicated that ENISA had achieved "Supporting cooperation in the cybersecurity community e.g. though private-public cooperation, information sharing, enhancing community building".
    - "Other" respondents (85% or 22) most frequently indicated that ENISA had achieved "Developing and maintaining a high-level of expertise in cybersecurity".
- Respondents were asked to comment on what they perceived as ENISA's main achievements over 2013-2016. In total 55 open responses were received of which 13 came from national authorities, 20 from private enterprises and business associations and 22 from "other" respondents. Respondents from all groups perceived the following as ENISA's main achievements:
    - The coordination of the Cyber Europe exercises.
    - The provision of support to CERTs/CSIRTs through training and workshops fostering coordination and exchange.
    - ENISA's publications that were considered as useful to create and update national security frameworks, as well as for reference to policy makers and cyber practitioners.
    - Assisting with the work under the NIS Directive.
    - Efforts to increase awareness on cybersecurity via the European Cybersecurity Month.

3. *Coherence of ENISA's activities with those of other organisations*

- 83% respondents considered ENISA's activities to be to a "large extent" or to "some extent" coherent with the policies and activities of their organisation (i.e. take into account, do not overlap, do not conflict with).

4. Location and organisational structure

- Respondents were asked whether they felt that ENISA's split location between Heraklion and Athens affected its ability to conduct its work effectively and efficiently. There were mixed perceptions expressed in relation to this question with 28% judging that the split location affected ENISA's ability to conduct its work effectively and efficiently to "some extent" or to "a large extent", while 20% stated "not at all".

Main results related to the forward looking questions:

- Respondents identified a number of gaps and challenges for the future of cybersecurity in the EU, in particular the top 5 (in a list of 16) were: cooperation across Member States in matters related to cyber security; capacity to prevent, detect and resolve large scale cyber-attacks; cooperation and information sharing between different stakeholders, including public-private cooperation; protection of critical infrastructure from cyber-attacks; skills development, education and training of professionals.

- A large majority (88%) of respondents considered the current instruments and mechanisms available at EU level to be insufficient or only partially adequate to address these. A large majority of respondents (98%) saw a need for an EU body to respond to these needs and among them ENISA was considered to be the right organisation to do so by 99%.

Main results related to the forward looking questions regarding specific topics:

1. Future needs and challenges

- Respondents were asked to select the most urgent needs or gaps in the cyber security field in the EU over the next ten years among a list of 16 needs and gaps. From the assessment made by 84 respondents, the largest number of respondents identified "Cooperation across Member States in matters related to cyber security" and the "Capacity to prevent, detect and resolve large scale cyber-attacks" as a main gap or need in the cybersecurity field in the EU over the next ten years. A majority of respondents within each respondent category (i.e. national authorities, private enterprise or business association and "other") identified these as needs or gaps.

- The views of the different respondent groups in relation to each of the options were relatively balanced, with the notable exception - among the most referred to gaps or needs – of "Cooperation and information sharing between different stakeholders, including public-private cooperation" where only two national authority respondents (out of a total of 14 national authority respondents) identified it as one of the most urgent needs or gaps.

- 55 respondents elaborated further on their answers to the question of what the most urgent needs or gaps in cybersecurity field will be in the next ten years. Out of the respondents to this open question, six were national authorities, 21 represented private enterprises or business associations, and 29 belonged to the group of "other" respondents. The contributions below represent the responses of all respondents given that little to no divergence was found in the answers among the different respondent categories:

    - Respondents commenting on the need for increased cooperation across Member States suggested that cooperation was necessary not only to bridge the security gaps that arise from a lack of cross-country cooperation, but also to build trust and confidence within the EU in matters of cybersecurity. Some respondents pointed to additional benefits of such cooperation, including increased market integration through the provision of internet services, support to the increase in cybersecurity capacity of less advanced Member States, and innovation for responses to current and future threats.

    - Closely linked to the identified need for cooperation were the identified needs for harmonised standards and certification in the field of cybersecurity, where respondents stated that the establishment of a common certification framework would help bridge inconsistencies and gaps in the implementation of security controls as well as to achieve trust across Europe.

    - Comments on the need to increase capacity to prevent, detect and resolve attacks pointed to the fact that the EU should step up the detection and real-time response to cyberattacks in information, communication technology (ICT), critical infrastructures, SMEs, government and public agencies.

    - Another largely discussed need or gap relates to skills development and education in the field of cybersecurity. Respondents commenting on this priority saw the need to increase the skills for cybersecurity professionals, particularly to address the changing market needs where industries increasingly need a highly skilled workforce. Respondents further commented that increasing citizen awareness on the importance of cybersecurity was a gap to be necessarily filled in given that "the human element" is the weakest link in cybersecurity.

- In this context, respondents from the groups of private enterprises and business associations and "other" respondents proposed a set of roles that ENISA could take on to address the identified needs or gaps. These included:
    - Promote coordination among EU institutions, Member States and the private sector, facilitating cooperation and effective flow of threat and incident information for swift responses and adaptation of security defensive solutions.
    - Support towards Member States to further cybersecurity research.
    - support the harmonisation of standards and certification by promoting existing internationally agreed standards and frameworks.
    - support government efforts related to the development of cybersecurity workforce through the development of guidelines-supporting cybersecurity experts across Europe.
    - ensure that the NIS Directive transposition across Member States is homogeneous.
- Respondents were also asked if the current instruments and mechanisms at the European level are adequate to promote and ensure cybersecurity in relation to the needs previously identified. Only 6% of the respondents judged the current instruments and mechanisms at the European level (such as regulatory framework, cooperation mechanisms, funding programmes, EU agencies and bodies) to be "fully adequate" to promote and ensure cybersecurity. 83% of respondents regarded them as either "partially" or only "marginally adequate" and 5% found them "not at all adequate". National authority respondents appear to be more positive about the adequacy of these instruments and mechanisms in comparison with representatives of private enterprises or business associations and "other" respondents.
- Based on the identified needs or gaps, respondents were asked what the priorities for EU action should be from now on and select up to three responses out of a list of 15. "Stronger EU cooperation mechanisms between Member States, including at operational level" was most frequently selected as a top priority, followed by "Stronger public-private cooperation in cybersecurity" and "improving research to address cybersecurity challenges".

2. The role of an EU body in the future EU cybersecurity landscape

- 98% of respondents saw a role for an EU-level-body in improving cybersecurity across the EU. Furthermore, almost all of the respondents (81 out of 82) who saw a role for an EU-level body in improving cybersecurity considered that ENISA could fulfil a role in bridging the different gaps in the future.

- Respondents have given examples of what ENISA's future role could be in addressing identified gaps and needs. The role seen for ENISA covered the following activities: fostering cooperation between Member States at international level and between the public and private sector; having a stronger role in policy development and implementation; ensuring harmonisation of approaches and setting baselines; certification and standardisation; providing incident response information; ensuring awareness raising, training and capacity building; supporting the private sector; ensuring the transposition of the NIS Directive; and fostering research. These activities were suggested by all respondent groups. Some national authorities underlined that ENISA should not take on an operational role in providing incident response activities, considering potential overlaps with CERT-EU and the need for the Agency to focus its resources on its core activities.

18.2. Results of the survey to CERT / CSIRT

The survey was conducted in January 2017 and targeted CERT / CSIRT representatives from all 28 Member States.

28 respondents completed the survey and 7 partially completed it. 1 partially completed response was deleted as it only answered the first question of the survey. The other partially completed answers were kept as they answered all of the mandatory questions except the ones in the section on "degree of coherence and complementarity".

Main results:

- 88% of respondents assessed that ENISA proactively supported cooperation among CERTs/CSIRTs to some or high extent during the 2013-2016 period. 82% of respondents assessed that ENISA covered the needs of the CERTs/CSIRTs to some or high extent.

- A very large majority (97%) expressed the view that ENISA's capacity building activities (e.g. training, National Cybersecurity Strategy support, identification of good practices) for CERTs/CSIRTs' development were either important or very important.

- Looking at the future, 85% of respondents assessed that the new roles foreseen for ENISA by the NIS Directive would enable ENISA to better cover CERTs/CSIRTs' needs to either some or high extent.

- Respondents were asked to provide more details, in concrete terms, of what they would foresee ENISA doing as part of its new role as secretariat for the CSIRTs Network (as foreseen in the NIS Directive); 16 respondents provided answers in the following categories:
  - Facilitating cooperation (standardization in data sharing at EU level; providing the link between the Cooperation and CSIRT Network Groups ; coordination of the CSIRTs' network activities)
  - Direct Support (e.g. contributing to the work program development)
  - Helping CERTs implement the NIS Directive (e.g. providing best practice recommendations on technical, organisational and legal issues concerning CSIRTs)
  - Capacity Building
  - Understanding Needs

18.3. Results of the survey to ENISA's staff and direct stakeholders

The survey addressed to ENISA's staff and direct stakeholders took place in January 2017.

The link to the survey was sent to a total of 173 stakeholders. We obtained 106 responses made up of 83 complete answers and 23 partially complete answers. Only the partially completed answers which responded to 50% or more of the mandatory questions were taken into account for the analysis. This led to a total of 88 answers, of which 83 were complete answers and 5 were partially completed answers. The responses provided a good representation of ENISA staff, Management and Executive Board members (71%) as well as Permanent Stakeholder Group (PSG) and Network of Liaison Officers (NLOs) representatives (29%).

Main results:

1. ENISA's organisational set-up
   - When asked whether the size of the Agency is appropriate for the work entrusted to ENISA and adequate for the actual workload, the majority of respondents gave a negative opinion: 14.8 % not at all; 36.4% to a limited extent; 30.7% to some extent. Respondents provided similar views across all categories; however ENISA staff (including management) were slightly more negative than Management Board (MB), Executive Board (EB), PSG and NLOs.

- The majoirty of ENISA staff found that the recruitment and training procedures are appropriate for the work entrusted to ENISA and adequate for the actual workload only to a limited extent (20.5%) or some extent (43.2%). The PSG expressed similar views, while Management Board and Executive Board were more positive, with almost 90% considering the recruitment and training procedures adequate to some or high extent.
- The staff composition was judged adequate to some or high extent by the majority of respondents (64.8%), with similar opinions expressed across all categories of respondents.

2. ENISA's effectiveness and efficiency
   - The majority of respondents (85,2%) found that the current governance structure, with a Management Board, an Executive Board and the Permanent Stakeholder Group, is conducive to the effective and efficient functioning of the Agency to some or high extent. The respondents from the Management Board, Executive Board and PSG were slighlty more positive than the ENISA staff and the NLOs.
   - The establishment of an Executive Board was found to lead to a more efficient functioning of the Management Board. This view has been supported in particular by the representatives of the MB and EB, while about 40% of the representatives of the staff, the PSG and NLOs said they did not know.
   - ENISA's management practices are considered conducive to creating an effective and efficient organisation to some or high extent respecitvely by 73% and 74% of respondents across all categories. ENISA's staff was slightly more critical than the other categories: 7% of the respondents found the management practices not at all conducive of effectiveness.
   - The questions on whether ENISA's location enables it to effectively (i.e. in terms of meeting its objectives) and efficiently conduct its work received mixed feedback. With regard to effectiveness respondents replied: not at all (11.4%); to a limited extent (17.0%); to some extent (27.3%); to high extent (39.8%). ENISA staff was proportionally more positive than the other categories of respondents; for example, 42% of respondents from the Management Board replied "not at all" or "to a limited extent". The same trend was found in the question related to the efficiency of the location: 11,4 % replied "not at all", 23,9% "to a limited extent"; 23,9% "to some extent", 35,2% "to a high extent". Again, ENISA staff was found to reply more positively than the other categories of respondents.

3. ENISA's relationship with stakeholders:
   - The vast majority (93%) expressed the views that ENISA to some or high extent has built strong and trustful relationships with its stakeholders when executing its mandate.

- 94% of respondents found that ENISA's activities are coherent with the policies and activities of its stakeholders. Respondents across all categories expressed similar views.

18.4. Results of the workshop on the future contribution of ENISA to EU cybersecurity

The workshop took place on 22 March 2017 in Brussels at the premises of DG Connect.

The workshop hosted a variety of stakeholders to enable engaging discussions. A group of 48 stakeholders included representatives of the Commission, members of ENISA's Management and Executive Board, as well as members ENISA's permanent stakeholder's group (PSG), representatives from national cybersecurity authorities and CERTs, industry representatives and academia.

The workshop was an opportunity to actively engage with them to discuss, qualify and validate the preliminary findings of the draft interim report on the "Study on the Evaluation of the European Union Agency for Network and Information Security" and to discuss the policy options for the future of ENISA. By discussing key findings with stakeholders, an assessment of findings and additional insights were gained contributing to the data collection and analysis of the study. The group also discussed the perceived needs in Europe in the area of cybersecurity.

Main results:

- The workshop participants identified the following four high relevance objectives for the work of the Agency:
  - Developing and maintaining a high level of expertise of EU actors.
  - Assisting Member States and the EU institutions in developing policies necessary to meet the regulatory requirements of NIS.
  - Assisting Member States and the Commission in enhancing capacity building throughout the EU.
  - Stimulating cooperation both between EU Member States and between related NIS communities.

- The workshop participants assessed that the ENISA mandate was highly relevant butthe actual activities did not fully meet the needs of the community. The main limitations noted were the fixed term ENISA mandate; limited ENISA's in-house expertise; limited ENISA's visibility; and limited resources.

- The workshop participants assessed that ENISA's main added value is the ability to enhance cooperation between Member States and NIS communities.

- A discussion took place on the possible options for the future of ENISA. Four options were presented (Keeping the status quo; Terminating ENISA; Strengthening ENISA with changes to its mandate; Establishing an EU cybersecurity centre). Following the discussion workshop participants indicated the option to strengthen ENISA with changes to its mandate as the favourite one. It was, however, indicated that the option of establishing an EU cybersecurity centre should have been further investigated.

19. SUMMARY OF RESULTS FROM THE CONSULTATIONS REGARDING ICT SECURITY CERTIFICATION FRAMEWORK

19.1. Results of the public consultation on the contractual public-private partnership on cybersecurity and accompanying measures related to ICT security certification

The public consultation on the contractual Public Private Partnership on cybersecurity took place from 18 December 2015 to 11 March 2016.

Respondents represented a wide variety of organisations, with a good balance between big business (41), SMEs (33), microbusiness (6) as well as other stakeholders e.g. research bodies (20), national public administrations (7) and regulators (1), NGOs (13).

Main results related to certification:

1. When answering the question whether national certification schemes are mutulally recognised across EU Member States 50,4% (121 out of 240) of respondents stated they "did not know", 25.8% (62 out of 240) replied 'No', while 23.8% (57 out of 240) replied 'Yes'.

2. 37,9% of respondents (91 out of 240) think the **existing certification schemes do not support the needs of Europe's industry**. On the other hand, 17, 5% (42 out of 240) – mainly global companies operating on the European market - expressed the opposite view.

3. 49.6% (119 out of 240) of respondants says that it is not easy to demonstrate equivalence between standards, certification schemes, and labels. 37.9% (91 out of 240) replied 'I do not know'.

In comments to the open question, some respondents emphasize that no reliable certification scheme exists at the moment at the European level, some others point also to the fact that existing national schemes act as barriers to market entry, complaining about the costs of complying with several certification schemes in Europe. Some of the industry associations state that **further fragmenting of the market** with numerous certification schemes **should be avoided**.

At the same time, some industry players emphasize the risk for companies of being overburdened with yet another certification scheme and therefore suggest a cautious approach to any new initiatives in this regard.

With regard to the EU cybersecurity industry, the majority of respondents view the European market as insufficiently competitive. Among the main weaknesses identified are different rules to access public procurement and fragmentation of EU market (in terms of cybersecurity requirements). In particular:

4. More than **44.3%** of respondents (78 out of 176) stated that they **experience barriers** related to market access and export within the EU and/or beyond EU countries, particularly due to the fragmentation of the EU cybersecurity market along EU internal borders.

5. Some respondents also pointed out that the lack of a European certification scheme and the emergence of national schemes, is factor that force them to go through **different costly and complex procedures**.

19.2. Results of the Workshops on 'The development of a European ICT Security Certification Framework'

The series of workshops presented below served as a follow-up on the Commission's commitment to consult stakeholders in the process of developing a proposal for a European ICT security certification framework as stated in Commissions' COM(2016) 410.

19.2.1. Workshop 1: October 2016

The Commission (DG CNECT, JRC) together with ENISA organised a workshop aiming at bringing together representatives from Member States to discuss the development of a possible ICT security certification of products and services. 15 representatives of Member States took part in the workshop. This workshop was a continuation of previous event on the topic of security certification. organised by ENISA in February and March 2016.

Main conclusions:

- A majority of national delegates welcomed the initiative of the Commission in the area of ICT security certification. In particular, they stressed the need to foster harmonization of security requirements at the European level.
- A roadmap indicating next steps for the development of European security certification framework was to be elaborated.
- A future certification framework should be based on different levels of certification including self-certification.
- It is necessary to harmonize evaluation methodologies across European labs.
- Any certification initiative should build as much as possible on the existing mechanism and international standards.

19.2.2. Workshop 2: December 2016

On 5 December 2016, the Commission and ENISA organised a follow-up workshop aiming at bringing together representatives from Member States to discuss the development of a possible ICT security certification of products and services. This workshop built on the discussion of the previous workshop (October) and saw the participation of 18 representatives from Member States.

A draft Roadmap - previously circulated by email – was further discussed during the workshop. While agreeing on the need to harmonize rules for ICT certification procedures at the European level, Member States called for greater clarity on key issues such as: Definition of scope of the overall initiative (e.g. products vs services, products category, sector)

Main conclusions:

- It was recommended that the Commission and Member States should: a) identify key sectors or product category; b) define fundamental principles for security certification in Europe; c) consider a pilot project that can help provide the skeleton of a future European certification and labelling Framework, identify initial priorities, estimates, resource allocation and timing.

- The European framework should be based, as much as possible, on existing mechanism and internationally recognised standards.

Participants were asked to outline a number of key points that will feed in the upcoming activities leading to the development of the future framework. The following work items – not formally adopted – were identified:

- Existing initiatives and practises should be identified;

- Industry's point of view, through European Cybersecurity Organisation (ECSO), should also be taken into consideration;

- A master plan of all ongoing activities should be put together;

- Exceptions, due to high value/high risk should be clearly scoped and considered; and

- The aspect of liability should also be taken into account.

All participants were given the opportunity to provide a written contribution by the end of December 2016.

19.2.3. Workshop 3: April 2017

On 27 April 2017, the Commission and ENISA organized a workshop attended by 90 participants. This workshop was a follow-up on the Commission's previous workshops (October, December 2016) and saw the participation of representatives from industry as well as Member States.

The workshop consisted of a plenary session in which public and private sector organizations presented their views on the challenges of a European ICT security certification framework. In the afternoon session participants had the opportunity to discuss in small focus groups the four main policy options that were presented such as:

Option 0 - Do nothing: No EU policy initiative or action – baseline scenario

Option 1 - Soft law approach: The Commission to encourage and support national or industry initiatives

Option 2 - Extension of SOGIS agreement: Legislative proposal making MS participation to the SOG-IS agreement mandatory

Option 3 - European certification framework: EU-wide framework with its own scope, functioning and governance rules.

Main conclusions:

- Following the group discussion, there was an overwhelming support - from Member States (DE, FR, SE, NL, PL, UK, AT, IT) and industry – for the policy Option that proposes the creation of a European institutional framework for ICT certification that builds on existing ICT certification mechanisms (e.g. SOG-IS Mutual Recognition Agreement);

- However, many underlined the importance to allocate adequate resources in order to ensure an appropriate maintenance of such a Framework;

- For this purpose, it was stressed that an EU body/ Agency (e.g. ENISA) should help carry out secretarial tasks;

- Other Options: it emerged that "no-action option" is not an option. While being more cost-effective, a soft law approach will not tackle the issue of fragmentation caused by emerging national ICT certification schemes popping up across Europe;

- Some Member States (e.g. SE, UK) and industry (e.g., DigitalEurope) called for a European ICT security framework to be built, as much as possible, on internationally recognized standards for cybersecurity certification; and

- As the smart meters industry is exposed to many national ICT certification requirements, the presenter from the trade association (ESMIG) offered to become pilot industry in the context of the development of an EU-wide approach to ICT security certification.

19.3. Results of the ENISA Survey on ICT security certification in the EU

This targeted survey took place from 5 until 19 May 2017. It has been broadly publicised within the confined certification community. Total number of participants: 33.

Respondents, who addressed questions related to certification, included national authorities/agencies (14); manufacturer / provider of ICT of ICT products and services (9); User / Customer / Consumer of ICT products and services (3); security certification laboratory (1); other (6).

This survey aimed to consult these stakeholders on the issue of security certification and labelling and seek structured feedback against set policy options such as:

Option 0 - Do nothing: No EU policy initiative or action – baseline scenario

Option 1 - Soft law approach: The Commission to encourage and support national or industry initiatives

Option 2 - Extension of SOGIS agreement: Legislative proposal making MS participation to the SOG-IS agreement mandatory

Option 3 - European certification framework: EU-wide framework with its own scope, functioning and governance rules.

Main results:

- 57%, (19) is aware of multiple existing ICT security certification schemes across EU Member States for the same product or service
- 37%, (12) indicated that they were not aware of multiple ICT security schemes across EU, but they expressed their preparedness to accept one
- the respondents indicated that the main problems they have encountered when dealing with security certification include:
    - 72% (24) Cost
    - 57% (19) Duration of process
    - 51% (17) Lack of mutual recognition of certificates across Member States
    - 45% (15) Lack of a dedicated scheme to cyber -certify a specific product/service
    - 39 (13) Lack of certification support for the lifecycle of the product (e.g., incremental certification for software and hardware changes/updates)
    - 36% (12) Lack of transparency
- 90% (30) agreed that mutual recognition of ICT security certification schemes is desirable at European level.
- 81% (27) agreed also that certification and labelling can be effective tools to increase transparency about the level of security assurances of ICT products/services, and enhance trust across the Digital Single Market.

- However, it has been noted that a ranking of assurance levels with clear information is required as oversimplifying could introduce additional risks. In addition, certification and labelling should denote only baseline security requirements and should not deferment innovation or increase complexity.

- 66% (22) agreed on the need for greater efforts to promote ICT security certification
- 21% (7) stated that ICT security certification is a pure market issue and there is no need for additional support.
- 75% (25) identified the need for ICT security and labelling in the Internet of Things-domain, due to imminent ubiquity of IoT, issues of vulnerabilities and the required interoperability across different platforms.
- 66% (22) identified the need for ICT security certification in the Industrial Control System (ICS)-domain, due to the criticality of processes they support and the level of cyber threats they are exposed to.

Policy Options

- 33% (11) have seen favourably a generic European certification framework, laying down essential rules for mutual recognition of certificates issued.
- 18% (6) favoured the “Soft law approach", encouraging, supporting and to the extent possible coordinating the adoption and use of certification initiatives at European level
- 12% (4) were in favour of extending the SOG-IS MRA to all Member States and make it mandatory.
- 12% (4) opted for regulating the security of I CT products and services and specify essential security requirements for such products to be placed on the market. T
- The remaining respondents indicated that a mixed approach, from all the aforementioned options, should be the preferred path of action instead. They argued that mutual recognition of existing certification schemes and labelling programs can promote a robust Digital Single Market and support EU digital economy while an entirely new certification framework would not be able to scale with the changing security landscape and consider the state-of-the-art
- 45% (15) were in favour of exploiting the current SOG-IS MRA as the basis to build an EU-wide certification Framework, while 21% (7) stated otherwise and 34% (11) did not answer either positive or negative on the role of SOG-IS MRA.
- 66% (22) agreed that self-certification schemes could be considered a viable option to boost the level of cyber-security for selected product’ domains, especially for low assurance level products and should be considered as an integral part of the future EU certification framework, drawing also experience from existing market driven initiatives. Nevertheless, 24% (8) of the respondents disagree that self-certification should be considered, as it does not provide any assurance, there is no control and it is not sufficient unless there is a third party validating conformance
- 90% (30) indicated that the processes and tools used for security certification should be improved to ensure the required flexibility by allowing different level of assurance.

- 66% (22) were in favour of the introduction of a common label across the EU. Such label will indicate that the products have been certified within a certification scheme in accordance with EU rules and visualize that the characteristics of the products and services comply withspecific requirements. Nevertheless, the respondents who were not in favour of a common label (8), proposed a specific sectoral labelling or consider that it could be difficult for complex systems and/or it could also result in a false sense of security
- 78% (26) envisage a role for existing EU Commission's bodies and agencies (e.g. JRC, ENISA, ACER) in a possible future EU certification and labelling security framework. Among the respondents who did not see a role for existing EU Commission's bodies and agencies (4), supporting actions such as determining a minimum level of security per category of technology, issuing voluntary guidelines for both industry and consumers, were envisioned, without identifying the key EU body or agency.

19.4. Results of the SME survey on ICT security certification

The survey was carried out in June 2017[134]. As of 23 June 2017, 46 respondents have answered the survey. Below are the main preliminary results. Please note that the submission to the Regulatory Scrutiny Board took place on 28 June 2017 while the survey was still ongoing.

Main preliminary results:

- 40 out of 46 respondents think that ICT security certification is a valuable tool to reduce cyber vulnerabilities of ICT products or services (4 replied "no", 2 replied "I don't know").

- 35 out of 46 respondents believe that the creation of an EU-wide ICT certification framework based on mutual recognition could facilitate SMEs' access to public procurements across Member States (4 replied "no", 7 replied "I don't know").

- 39 out of 46 respondents would be in favour of a common label for certified ICT products (3 replied "no", 4 replied "I don't know").

- 35 out of 46 respondents consider that creating a European certification general framework laying down the essential rules for mutual recognition of certificates is an appropriate action to achieve the objective of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU (multiple answers question).

[134] Survey opening dates: 02-30 June 2017. The survey can be found at: https://ec.europa.eu/eusurvey/runner/ICTCertificationSecurityFramework.

- 24 out of 46 respondents consider that regulating the security of ICT products and services, specifying essential security requirements for such products to be placed on the market is an appropriate action to achieve the objective of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU (multiple answers question).

- 20 out of 46 respondents see the emergence of multiple national or sectorial certification schemes as a likely scenario in the future, especially in view of the growing cybersecurity risks (8 replied "no", 12 replied "I don't know").

- Two-thirds (30 out of 46) respondents think that a mutual recognition mechanism of certificates across all Member States can be useful to simplify procedures and cut administrative burdens for them (multiple answers question).

- Two-thirds (30 out of 46 respondents) think that a mutual recognition mechanism of certificates across all Member States could be useful to reduce cost of compliance for them (multiple answers question).

- More than half (25 out of 46 respondents) believe that self-certification schemes are NOT a viable option to boost the level of cybersecurity for selected product' domains (17 replied "yes", and 4 replied "I don't know").

- 37 out of 46 respondents think that the processes and tools used for ICT security certification should be sufficiently flexible and take into account different levels of assurances according to market needs (6 replied "no" and 3 replied "I don't know").

- 34 out of 46 respondents are of the opinion that a labelling scheme underlying the level of security and privacy an IoT device encompasses would help them increase trust in IoT products and services (4 replied "no", 8 replied "I don't know").

- 34 out of 46 respondents identified the cost of current ICT security certification procedures as a problem they encountered (multiple answers question).

- 28 out of 46 respondents identified the duration of the process of current ICT security certification procedures as a problem they encountered (multiple answers question).

- 18 out of 46 respondents believe that the current existence of multiple ICT certification schemes represents a barrier to market entry for them because they are too costly and therefore not affordable for SMEs (most respondents left question 6 blank, 6 replied "lack of reference levels").

- 25 out of 46 respondents said that the main reason that makes them reluctant to buy emerging digital technology products and services is that they are afraid of the cybersecurity risks and consequent damages that may be brought to them (multiple answers question).

- 25 out of 46 respondents feel comfortable installing any software updates needed for the proper functioning of their connected device themselves (multiple answers question).

- 24 out of 46 respondents estimate the cost for certifying an ICT service or product to be between 10,000 and 100,000. 15 out of 46 estimated the cost to be between 100,000 and 1,000,000.

- 18 out of 46 respondents believe ENISA should promote certification schemes and identify the common standards (most didn't reply, 2 replied "ENISA should make sure competition is respected and that the market remains open").

ANNEX 3:

EU Agencies Budget and Staff

The table below provides information on the total EU financial contribution to 32 decentralised EU agencies, as well as their authorised establishment plans (i.e. staff) in 2017. The information derives from the "Draft General Budget of the EU for the financial year 2018 – Working Document Part III – Bodies set up by having legal personality and Public-Private Partnership"[135], unless otherwise stated.

No.	Agency	Total EU contribution (million EUR)	Authorised establishment plan (staff)[136]
1.	European Agency for the Management of Operational Cooperation at the External Borders – **FRONTEX**	281.267	352
2.	European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice – **EU-LISA**	153.334	131
3.	European Police Office – **EUROPOL**	114.624	550
4.	European Food Safety Authority – **EFSA**	77.333	323
5.	European Chemicals Agency – **ECHA**[137]	75.173	460
6.	European Maritime Safety Agency – **EMSA**	72.359	212
7.	European Asylum Support Office – **EASO**	69.206	155
8.	European Centre for Disease Prevention and Control – **ECDC**	56.766	182
9.	The European Union s Judicial Cooperation Unit - **EUROJUST**	48.379	208
10.	European Environment Agency – **EEA**	36.309	127
11.	European Aviation Safety Agency – **EASA**	35.985	678
12.	European Railway Safety Agency – **ERA**	30	139

[135] COM(2017) 400 – June 2017, available at: https://myintracomm.ec.europa.eu/budgweb/EN/bud/proc/adopt/Documents/DB2018-WD03-agencies.pdf.

[136] This category includes only permanent staff. It does not include contract agents and seconded national experts.

[137] This agency is partially self-financed.

No.	Agency	Total EU contribution (million EUR)	Authorised establishment plan (staff)[136]
13.	European Medicines Agency – **EMA**	28.892	596
14.	European GNSS Agency – **GSA**[138]	27.847	116
15.	European Union Agency for Fundamental Rights – **FRA**	22.567	72
16.	European foundation for improvement of living & working conditions – **EUROFOUND**	20.371	93
17.	European Training Foundation – **ETF**	20.144	88
18.	European Centre for the Development of Vocational Training – **CEDEFOP**	17.434	92
19.	European Fisheries Control Agency – **EFCA**	17.113	61
20.	European Monitoring Centre for Drugs and Drug Addiction – **EMCDDA**	15.136	77
21.	European Agency for Safety and Health at Work – **EU-OSHA**	14.679	40
22.	European Banking Authority – **EBA**[139]	14.543	134
23.	European Agency for the Cooperation of Energy Regulators – **ACER**	13.272	68
24.	European Securities and Markets Authority – **ESMA**	11.02	150
25.	**European Network and Information Security Agency – ENISA**	**10.322**	**48**
26.	European Police College – **CEPOL**	9.28	31
27.	European Insurance and Occupational Pensions Authority – **EIOPA**	8.946	101
28.	European Institute for Gender equality – **EIGE**	7.628	27
29.	Office of the body of European Regulators for Electronic Communications – **BEREC**	4.246	14
30.	Single Resolution Board – **SRB**[140]	0	350
31.	Community Plant Variety Office – **CPVO**[141]	0	44

[138] This excludes the amount delegated to GSA in 2017 and 2018.

[139] This agency is partially co-financed by national public authorities.

[140] This agency is fully self-financed and does not receive EU contribution.

[141] This agency is fully self-financed and does not receive EU contribution.

No.	Agency	Total EU contribution (million EUR)	Authorised establishment plan (staff)[136]
32.	European Union Intellectual Property Office – **EUIPO**[142]	0	792

***

[142] This agency is fully self-financed and does not receive EU contribution.

Annex 4: Preliminary mapping of the EU-level entities that provide cybersecurity content

The tables below provide a first listing of the EU level entities that provide cybersecurity related information, the type of information, the target audience and the frequency with which they convey such information.

This preliminary mapping was provided by the Commission DG Joint Research Centre (JRC) as part of a technical report on the possible requirements of a European Cybersecurity Information Hub.

Acronym	Description
CERT-EU	After a pilot phase of one year and a successful assessment by its constituency and its peers, the EU Institutions have decided to set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies on September 11th 2012. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies.
	https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html
ENISA	The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. ENISA is contributing to a high level of network and information security (NIS) within the European Union, by developing and promoting a culture of NIS in society to assist in the proper functioning of the internal market
	https://www.enisa.europa.eu/
ERNCIP	European Reference Network for Critical Infrastructure Protection (ERNCIP). aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards and to the creation of a single market for security solutions.
	https://ec.europa.eu/jrc/en/network-bureau/european-reference-network-critical-infrastructure-protection-erncip
ETSI	ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. Our standards enable the technologies on which business and society rely. For example, our standards for GSM™, DECT™, Smart Cards and electronic signatures have helped to revolutionize modern life all over the world.
	http://www.etsi.org/
CENELEC	CENELEC is the European Committee for Electrotechnical Standardization and is responsible for standardization in the electrotechnical engineering field. CENELEC prepares voluntary standards, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market.
	https://www.cencenelec.eu/Pages/default.aspx
Eurolex	EUR-Lex provides free access, in the 24 official EU languages, to: the authentic Official Journal of the European Union EU law (EU treaties, directives, regulations, decisions, consolidated legislation, etc.) preparatory acts (legislative proposals, reports, green and white papers, etc.) EU case-law (judgments, orders, etc.) international agreements EFTA documents summaries of EU legislation, which put legal acts into a policy context, explained in plain language other public documents.
	http://eur-lex.europa.eu/homepage.html
STOA	European Parliament Science and Technology Options Assessment (STOA) The STOA Panel forms an integral part of the structure of the European Parliament. It is composed of 25 Members of the European Parliament (MEPs) who are nominated by nine permanent Committees of the Parliament: AGRI, CULT, EMPL, ENVI, IMCO, ITRE, JURI, LIBE and TRAN. The EP Vice-President responsible for STOA is a Member of the Panel ex officio. The members of the STOA Panel are appointed for a renewable two-and-a-half-year period.
	http://www.europarl.europa.eu/stoa/
SAM	Scientific Advice Mechanism: Scientific advice in the area of cybersecurity has been requested by Vice President Ansip and Commissioner Oettinger during the SAM High Level Group first meeting on 29 January 2016. The corresponding scoping paper outlines the issues at stake, the EU policy landscape and the potential areas for scientific advice to inform policy-making
	https://ec.europa.eu/research/sam/index.cfm?pg=cybersecurity
ACER	ACER's missions and tasks are defined by the Directives and Regulations of the Third Energy Package, especially Regulation (EC) 713/2009 establishing the Agency. In 2011, ACER received additional tasks under Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT) and in 2013 under Regulation (EU) No 347/2013 on guidelines for trans-European energy infrastructure. The Agency's overall mission, as stated in its founding regulation, is to complement and coordinate the work of national energy regulators at EU level, and to work towards the completion of the single EU energy market for electricity and natural gas. ACER plays a central role in the development of EU-wide network and market rules with a view to enhancing competition. The Agency coordinates regional and cross-regional initiatives, which favour market integration. It monitors the work of European networks of transmission system operators (ENTSOs), and notably, their EU-wide network development plans. Finally, ACER monitors the functioning of gas and electricity markets in general, and of wholesale energy trading in particular.
	http://www.acer.europa.eu/
EDPS	The European Data Protection Supervisor (EDPS) is the European Union's (EU) independent data protection authority. It's general mission is to: monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals; advise EU institutions and bodies on all matters relating to the processing of personal information. It is consulted by the EU legislator on proposals for legislation and new policy developments that may affect privacy; monitor new technology that may affect the protection of personal information; intervene before the Court of Justice of the EU to provide expert advice on interpreting data protection law; cooperate with national supervisory authorities and other supervisory bodies to improve consistency in protecting personal information.
	https://edps.europa.eu/
JRC	As the European Commission's science and knowledge service, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle. Its work has a direct impact on the lives of citizens by contributing with its research outcomes to a healthy and safe environment, secure energy supplies, sustainable mobility and consumer health and safety.
	https://ec.europa.eu/jrc/en
Europol	Europol assists the 28 EU Member States in their fight against serious international crime and terrorism. Europol also works with many non-EU partner states and international organisations.
	https://www.europol.europa.eu/
DG-ENER	The Directorate-General for Energy is one of 33 policy-specific departments in the European Commission. It focuses on developing and implementing the EU's energy policy – secure, sustainable, and competitive energy for Europe. The Directorate General develops and implements innovative policies aimed at: i) contributing to setting up an energy market providing citizens and business with affordable energy, competitive prices and technologically advanced energy services, ii) promoting sustainable energy production, transport and consumption in line with the EU 2020 targets and with a view to the 2050 decarbonisation objective, iii) enhancing the conditions for safe and secure energy supply in a spirit of solidarity between EU countries ensuring a high degree of protection for European citizen
	https://ec.europa.eu/energy/en
ECSO	The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016. ECSO represents an industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity, and in particular to: Foster and protect from cyber threats the growth of the European Digital Single Market; Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position; Develop and implement cybersecurity solutions for the critical steps of trusted supply chains, in sectoral applications where Europe is a leader.
	https://www.ecs-org.eu/
IOTA	The Internet of Things Association is an industry forum hosted by Smartex, not an EU body
	http://www.smartex.com/IOTA/
Working Group Art. 29	The Working Party was set up to achieve several primary objectives: To provide expert opinion from member state level to the Commission on questions of data protection; To promote the uniform application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities; To advise the Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy; To make recommendations to the public at large, and in particular to Community institutions on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community.
	http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Entity	Type of Content			Domain	Nature	Target Audience	Access Media		
	Knowledge	Services	Software Tools				Web portal	Mobile phone app	Social Media
CERT-EU	White papers/Guidelines, Software vulnerabilities, Web articles	Monitoring of cybersecurity news using European Media Monitor (EEM)		Information Systems	Technical	General	X	X	
ENISA	Best practices & recommendations, Standards and certifications	Training of cyber security specialists, Cyber Exercises and Cyber Security Education, Trust services, Incident Reporting		Cloud and Big Data, Critical Infrastructure and Services, Cyber Crisis Management, IoT and Smart Infrastructures, Data protection, National Cyber Security Strategies, Threat and risk management	Technical	General	X		Twitter, Facebook, LinkedIn, Youtube
ERNCIP	Requirements and Guidelines	Certification		Critical Infrastructures and Industrial Automation and Control Systems		Industry	X		
ETSI	Standards and White papers			Telecommunication system	Technical	Industry	X		Twitter, Facebook, LinkedIn, Google+, Youtube
CENELEC	Standards and Guidelines			Electrotechnical engineering	Technical	Industry	X		Twitter, Facebook, Linkedin, YouTube
Eurolex	Directives and Regulation			General purpose	Legislation	General	X		
STOA	Studies			General purpose	Scientifical	Government Institutions	X		Twitter, Facebook
SAM	Observations, Recommendations, and Scientific opinions			General purpose in the EU policy landscape	Scientifical	Government Institutions	X		
ACER	Recommendations, Guidelines, and Opinions			Energy infrastructure	Technical	Industry and Government Institutions	X		
EDPS	Reference library, Annual Reports, Factsheets, Speeches and Articles, EDPS Strategy			Data protection	Technical	Industry and Government Institutions	X	X	Twitter, LinkedIn, Youtube
JRC	Publications, Technical Reports, Scientific Reports, Patents and Technologies	Science oriented policy support	Scientific Tools and Databases	General purpose in the EU policy landscape	Scientifical	General	X		Twitter, Facebook, LinkedIn, Youtube
Europol	Articles, Definitions, Public awareness and prevention guides, Reports	Threat assessments, Early warning notifications		Cybercrime and terrorism	Technical	General	X		Facebook, Twitter, Youtube, LinkedIn
DG-ENER	Studies, Consultations, Reports, Infographics			Energy infrastructure	Technical	Industry and Government Institutions	X		Twitter, Pinterest
ECSO	Reference Documents			Public-Private partnership	Technical	Industry	X		Twitter
IOTA				Internet of Things (IoT)	Technical	Industry	X		
Working Group Art. 29	Guidelines, Letters of members/chair, Opinions			Data protection	Legislation	General	X		