



Brussels, 16.12.2020  
SWD(2020) 345 final

PART 1/3

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT REPORT**

*Accompanying the document*

**Proposal for a Directive of the European Parliament and of the Council  
on measures for a high common level of cybersecurity across the Union, repealing  
Directive (EU) 2016/1148**

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 344 final}

## Table of contents

1.	Introduction .....	9
1.1.	Political context and legal framework .....	9
1.2.	Results of the evaluation of the NIS Directive .....	13
2.	Problem definition .....	15
2.1.	What are the problems? .....	15
2.2.	What are the problem drivers? .....	23
3.	How will the problem evolve? .....	28
4.	Why should the EU act? .....	29
4.1.	Legal basis .....	29
4.2.	Subsidiarity: Necessity of EU action.....	30
4.3.	Subsidiarity: Added value of EU action .....	30
5.	Objectives: What is to be achieved?.....	31
5.1.	General objectives .....	31
5.2.	Specific objectives .....	32
6.	What are the available policy options?.....	32
6.1.	Description of the policy options .....	32
6.2.	Options discarded at an early stage .....	69
7.	What are the impacts of the policy options? .....	70
7.1.	Economic impact and efficiency .....	70
7.2.	Social impacts.....	88
7.3.	Environmental impacts .....	88
7.4.	Impacts on fundamental rights .....	88
8.	How do the options compare? .....	89
9.	Preferred option .....	92
9.1.	Rationale and benefits of the preferred option .....	92
9.3.	REFIT (simplification and improved efficiency) .....	93
10.	How will actual impact be monitored and evaluated?.....	95

## Glossary: acronyms

<i>Term or acronym</i>	<i>Meaning</i>
AI	Artificial Intelligence
CDN	Content delivery network
CSIRTs	Computer Security Incident Response Teams
CyCLONe	European Cyber Crises Liaison Organisation Network
DDoS	Distributed Denial of Service
DEP	Digital Europe Programme
DESI	Digital Economy and Society Index
DNS	Domain Name System
DORA	Digital Operational Resilience Act for the financial sector
DSP	Digital service provider
EASA	The European Union Aviation Safety Agency
ECCSA	European Centre for Cybersecurity in Aviation
ECI Directive	Directive on the identification and designation of European critical infrastructures
ECJ	European Court of Justice
EECC	European Electronic Communications Code
EMSA	European Marine Safety Agency
eIDAS (Regulation)	Regulation on electronic identification and trust services for electronic transactions in the internal market

ENISA	The European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a service ( <i>cloud service model</i> )
ICS	Industrial control system
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union: The United Nations specialised agency for information and communication technologies
IXPs	Internet Exchange Points
JRC	European Commission's Joint Research Centre
LOTL	European List of eIDAS Trusted Lists
OES	Operator of essential services
OPC	Open public consultation
MeliCERTes	Cybersecurity Digital Service Infrastructure Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs
NACE	Statistical Classification of Economic Activities in the European Community
NIS Directive	Directive concerning measures for a high common level of security of network and information systems across the Union
NIST	National Institute of Standards and Technology – US

	Department of Commerce
PaaS	Platform as a Service ( <i>cloud service model</i> )
PPP	Private Public Partnership
ROSI	Return of Security Investment
SaaS	Software as a Service ( <i>cloud service model</i> )
SME	Small and medium-sized enterprises
SPOC	Single Point of Contact
TFEU	Treaty on the Functioning of the European Union
TLD	Top-level domain

*Glossary: terms and definitions*

<i>Term/concept</i>	<i>Definition</i>
ARGUS	General rapid alert system linking all the European Commission's specialised systems for emergencies
Cloud computing service	A digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources
Content delivery network	A network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and services to internet users on behalf of content and service providers
Cybersecurity	The activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats
Cybersecurity certification scheme	A comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a public authority and that apply to the certification or conformity assessment of ICT products, ICT services and ICT processes falling under the scope of the specific scheme
Cyber threat	Any potential circumstance, event or action within the meaning of point 8 of Article 2 of Regulation (EU) 2019/881
Data centre service	A service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network telecommunications equipment providing data storage, processing and transport services together with all the facilities and infrastructures for power distribution and environmental control
Distributed denial-of-service (DDoS) attack	A malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic
Domain name system (DNS)	A hierarchical distributed naming system which allows end-users to reach services and resources on the open internet
DNS service provider	An entity that provides recursive or authoritative domain name resolution services to internet end-users and other DNS

	service providers based on information contained in the hierarchical structure of the DNS
Edge computing	Distributed, open IT architecture that features decentralised processing power, enabling mobile computing and Internet of Things (IoT) technologies. In edge computing, data is processed by the device itself or by a local computer or server, rather than being transmitted to a data centre
Incident	Any event compromising the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, network and information systems
Incident handling	All procedures supporting the detection, analysis and containment of an incident and the response thereto
Internet exchange point (IXP)	A network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic
ISO 27000-series standards	Series of mutually supporting information security standards that can be combined to provide a globally recognised framework for best-practice information security management
NIST standards	Standards aimed at driving innovation and economic competitiveness at U.S.-based organizations in the science and technology industry developed by the National Institute of Standards and Technology (NIST). NIST standards are based on best practices from several security documents, organizations, and publications, and are designed as a framework for federal agencies and programs requiring stringent security measures
Network and information system	An electronic communications network or any device or group of inter-connected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data, or digital data stored, processed, retrieved or transmitted by elements covered under the previous points for the purposes of their operation, use, protection and maintenance

Online marketplace	Digital service that allows consumers and/or traders to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace
Online search engine	A digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found
Operators of government-owned and privately-owned ground-based infrastructure that support the provision of space-based services	Ground-based government-owned and privately-owned infrastructure that supports the provision of space-based services, with the exception of specific ground-based infrastructure that directly supports space-based components of the EU's space programme, including Galileo, EGNOS, Copernicus, GOVSATCOM and Space Surveillance and Tracking
Provision of an electronic communications network	The establishment, operation, control or making available of such a network, as defined by the Directive (EU) 2018/1972 establishing the European Electronic Communications Code
Public electronic communications networks or of publicly available electronic communications services	Electronic communications network used wholly or mainly for the provision of publicly available electronic communications services which support the transfer of information between network termination points, as defined by the Directive (EU) 2018/1972 establishing the European Electronic Communications Code
Public administration entities	Public entities that: (i) are established for the purpose of meeting needs in the general interest and does not have an industrial or commercial character; (ii) have legal personality; (iii) are financed, for the most part, by the State, regional authority, or by other bodies governed by public law; or is subject to management supervision by those authorities or bodies; or have an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional authorities, or by other bodies governed by public law and (iv) have the power to address to natural or legal persons administrative or regulatory decisions affecting their rights in the cross-border movement of persons, goods, services and capital.
Ransomware	Type of malware (e.g. viruses, trojans, etc.) 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 shortly after receives a blackmail note by pop-up, pressing the victim to pay a ransom to regain full access to system and files.
Security of network and information systems	The ability of network and information systems to resist, at a given level of confidence, any action, that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems
Social network	An online multi-sided platform that enables users to connect, share, discover and communicate with each other across multiple devices (mobile and desktop) and means (e.g., via chats, posts, videos, recommendations)
Top-level domain name registry	An entity which administers and operates a specific top-level domain (TLD) by providing the registration of domain names under the TLD and the technical operation of the TLD, including the operation of its name servers, the maintenance of its databases and the distribution of TLD zone files across name servers
Trust service provider	Trust Service Providers, within the meaning of Article 3(19) of the eIDAS Regulation, are responsible for assuring the digital ID of people through authentication, digital certificates and digital signatures
Vulnerability	A weakness, susceptibility or flaw of an asset, system, process or control that can be exploited by a threat
Waste water	Water that is of no further immediate value to the purpose for which it was used or in the pursuit of which it was produced because of its quality, quantity or time of occurrence.

## 1. INTRODUCTION

### 1.1. Political context and legal framework

The Directive concerning measures for a high common level of security of network and information systems across the Union<sup>1</sup> (hereinafter called the ‘NIS Directive’), which entered into force in August 2016, was the first piece of EU-wide legislation on cybersecurity. By now, all Member States have transposed the NIS Directive into national law.

Article 23(2) of the NIS Directive requires the Commission to review the functioning of the Directive by 9 May 2021. The review is also mentioned in the Adjusted Commission Work Programme 2020, which envisages a legislative proposal accompanied by an impact assessment in Q4 of 2020.<sup>2</sup> Furthermore, the **EU Security Union Strategy for 2020 to 2025**<sup>3</sup>, which focuses on priority areas where the EU can bring value to support Member States in fostering security, also comprises provisions on cybersecurity, mentioning the review of the NIS Directive planned to be completed by the end of 2020.

Cybersecurity is also one of the Commission’s priorities in its response to the COVID-19 crisis, and consequently the **Recovery Plan for Europe**<sup>4</sup> includes additional investments in cybersecurity. In its **Communication on Shaping Europe’s Digital Future** of February 2020, the Commission highlighted the need to cooperate with a view to “*setting consistent rules for companies and stronger mechanisms for proactive information-sharing; ensuring operational cooperation between Member States, and between the EU and Member States*”.<sup>5</sup>

At the level of the European Parliament, a resolution from 12 March 2019 called “[...] *on the Commission to assess the need to further enlarge the scope of the NIS Directive to other critical sectors and services that are not covered by sector-specific legislation*”.<sup>6</sup> The Council, in its conclusions from 9 June 2020, welcomed “[...] *the Commission’s plans to ensure consistent rules for market operators and facilitate secure, robust and appropriate information-sharing on threats as well as incidents, including through a review of the Directive on security of network and information systems (NIS Directive), to pursue options for improved cyber resilience and more effective responses to cyber-attacks, particularly on essential economic and societal activities, whilst respecting Member States’ competences, including the responsibility for their national security.*”<sup>7</sup>

The NIS Directive provided the **overall framework for cybersecurity cooperation at national and EU levels**. It has also served as a catalyst in many Member States, paving the way for a significant change in mind-set, institutional and regulatory approach to cybersecurity. In particular, it sets the basis for:

- (i). improved cybersecurity capabilities at national level by requiring Member States to draw up national strategies and appoint authorities with responsibility for cybersecurity.

---

<sup>1</sup> Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

<sup>2</sup> [https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents\\_en](https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents_en)

<sup>3</sup> COM(2020) 605 final, 24 July 2020.

<sup>4</sup> Special meeting of the European Council (17, 18, 19, 20 and 21 July 2020) – Conclusions: <https://www.consilium.europa.eu/en/press/press-releases/2020/07/21/european-council-conclusions-17-21-july-2020/>

<sup>5</sup> [https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020\\_en\\_4.pdf](https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf)

<sup>6</sup> [https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html)

<sup>7</sup> <https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf>

- (ii). increased EU-level cooperation through the creation of two new EU fora, both strategic and operational<sup>8</sup>, as well as exchange of information among Member States, mainly on a voluntary basis.
- (iii). requirements for Member States to define risk management (security requirements) and incident reporting obligations, notably for operators of essential services (hereinafter called ‘OESs’) in seven specific sectors, i.e. healthcare, transport, energy, banking, financial market infrastructure, drinking water supply and distribution and digital infrastructure, and digital service providers (hereinafter called ‘DSPs’), i.e. online marketplaces, online search engines and cloud computing services.

Through the Cooperation Group<sup>9</sup>, the NIS Directive also brought Member States’ authorities together and, despite some initial reluctance to engage at EU and cross-country level due to perceived national security sensitivities and lack of trust, it made everybody more aware of the need for unity and coordinated efforts as a pre-requisite for enhanced resilience against cybersecurity risks. The Cooperation Group therefore set up a solid basis for EU level cooperation on cybersecurity policy aspects, developing into an extensive setting where specific work streams focusing on a wide range of NIS-related aspects are constantly being consolidated and expanded. To illustrate this, the NIS Directive provided a structure and the Cooperation Group provided the forum for the work on 5G network security.<sup>10</sup> The network of national Computer Security Incident Response Teams (hereinafter called ‘CSIRTs’) facilitated some more operational exchanges among Member States. It is also within the NIS Directive’s cooperation framework that the Commission, with support from Member States, issued a blueprint for rapid emergency response in case of large-scale cross-border cyber incidents or crisis.<sup>11</sup> Based on this, Cyber Europe incident and crisis management exercises were developed and a Cyber Crises Liaison Organisation Network (“CyCLONe”) is being set up.

The entities subject to the NIS Directive’s requirements are as follows:

- operators of essential services (OESs) in the seven sectors mentioned above, as identified by the Member States. The companies active in these sectors must go through an identification process at Member State level, to establish whether they qualify as OESs within the NIS scope. The Member States also define the security requirements that OESs have to put in place and establish the concrete thresholds and procedures for incident reporting.
- digital service providers (DSPs) of the types mentioned above. These are not subject to an identification process, the maximum harmonisation principle applies to their obligations and they are subjected to a so called light-touch approach based on reactive *ex post* supervisory activity justified by the nature of their services and operations.<sup>12</sup> DSPs do not have to gather evidence on the implementation of security policies and the competent authorities should have no general obligation to supervise DSPs.

<sup>8</sup> via a Cooperation Group and a network of Computer Security Incident Response Teams – CSIRTs.

<sup>9</sup> The NIS Cooperation Group has been established by Article 11 of the NIS Directive to ensure strategic cooperation and the exchange of information among EU Member States in cybersecurity

<sup>10</sup> Notably for the implementation of the Commission Recommendation and the EU toolbox of risk mitigating measures. Cooperation Group publication of January 2020: <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures> .

<sup>11</sup> Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, C(2017) 6100 final.

<sup>12</sup> As stipulated by recital (60) of the NIS Directive.

As regards the supervision and enforcement framework, the NIS Directive contains general provisions, which neither specify minimum requirements for supervisory measures that can be applied by the competent authorities, nor set a minimum level of penalties for non-compliance with the obligations stipulated by the Directive.

However, in spite of the above-mentioned achievements, the NIS Directive also proved its limitations, falling short of ensuring a fully engaging, coherent and pro-active setting that could guarantee an effective take of **shared responsibilities** and **trust** among all relevant **authorities and businesses**. As shown by the evaluation of its functioning (*see Annex 5*), the NIS Directive revealed **inherent weaknesses and gaps** that make it incapable of addressing contemporaneous and emerging cybersecurity challenges. These concern, among others, the lack of clarity on the NIS scope, the insufficient consideration of the increasing interconnectivity and interdependencies within EU economies and societies, the lack of alignment of security requirements and reporting obligations, the lack of effective incentives for information sharing or operational cooperation among relevant authorities and the difference in treatment of comparable businesses across Member States and sectors. For example, as a result of some of these gaps, there are situations where major hospitals in a Member State do not fall within the scope of the NIS Directive and hence are not required to have in place the resulting security measures, while another Member State with a similar population size included under the NIS scope almost every single hospital in the country. Similarly, while a major European railway operator is included under the NIS scope in one big Member State, another major railway operator in another big Member State is not covered by the NIS security requirements.<sup>13</sup>

In addition, the speedy digital transformation of society has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. More advanced policy responses in the field of cybersecurity have become a matter of urgency, as the number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources inside and outside the EU. State or state-backed actors are frequently involved. There were almost 450 cybersecurity incidents in 2019 involving critical infrastructures in Europe like health, finance and energy.<sup>14</sup> One cyberattack alone can cause substantial damages across organisations, sectors, and citizens. For example, the economic impact of the 2017 WannaCry incident is estimated in the order of hundreds of million euros or even more. In its latest Global Risks Report, the World Economic Forum mentions cyberattacks as one of the top 10 risks by likelihood and by impact over the next 10 years.<sup>15</sup>

The COVID-19 crisis and the resulting sudden increase in demand for internet-based solutions has emphasised an even stronger need for a state of the art cybersecurity. The pressures of the COVID-19 outbreak have led to cyber-attacks exploiting the situation in different ways, from taking advantage of the intense pressure on hospitals<sup>16</sup>, to abusing the mass move to home digital working. Ransomware and distributed denial of service (DDoS) attacks remain a permanent threat, targeting key digital services like major cloud

---

<sup>13</sup> This information is based on the Member States' notifications of the number of OES identified, in line with Article 5(7)(c).

<sup>14</sup> <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>.

<sup>15</sup> World Economic Forum (2020): The Global Risks Report 2020 (<https://www.weforum.org/reports/the-global-risks-report-2020>)

<sup>16</sup> For example, a cyber-attack on Brno University Hospital Brno (Czechia) defined by Europol as an attack on critical health infrastructure (*Europol, Pandemic profiteering: How criminals exploit the COVID-19 crisis. March 2020*).

providers.<sup>17</sup> The move to connected devices will bring great benefits for users: but with less data stored or processed in data centres, and more processed closer to the user ‘at the edge’, cybersecurity will no longer be able to focus on protecting central points.<sup>18</sup>

Overall, since the implementation of the NIS Directive, European countries have become increasingly dependent on digital and information systems, while their networks have become ever-more interconnected. As highlighted by the **EU Security Union strategy**<sup>19</sup>, security threats are feeding more and more on the ability to work cross-border and on inter-connectivity, exploiting the blurring boundaries between the physical and digital world. To this end, while reviewing the NIS Directive, the Commission is also preparing a proposal, due by the end of 2020, for additional measures to enhance the protection and resilience of critical infrastructure, to replace the Directive on the identification and designation of **European critical infrastructures**<sup>20</sup> (hereinafter called ‘the ECI Directive’) with an **overarching cross-sectoral framework** focused on non-cyber threats. The current ECI Directive covers infrastructures the disruption of which would have an impact on at least two Member States in two sectors: energy and transport. It is envisaged to ensure greater coherence between the EU critical infrastructure protection and the NIS Directive, especially when it comes to the sectoral scope of both initiatives. The initiative considers introducing measures to enhance the resilience of critical infrastructures in the face of non-cyber risks.

**Sector-specific** initiatives are also addressing cybersecurity aspects, in synchronisation with the NIS framework. For example, the Network Code for the cybersecurity of cross-border energy flows, the rules for cybersecurity in the aviation security domain<sup>21</sup> and the Commission proposal for a Digital Operational Resilience Act for financial services<sup>22</sup> (DORA) provide sector-specific cybersecurity provisions. Finally, there is a number of related laws at EU level aiming to achieve complementary objectives, most notably the General Data Protection Regulation (GDPR), which contains provisions on the security of personal data for data controllers and processors, but also the e-Privacy Directive.<sup>23</sup> *See also Annex 7 on related policy and legislative initiatives, including the Regulation on electronic identification and trust services for electronic transactions in the internal market (hereinafter called the ‘eIDAS Regulation’)*<sup>24</sup> and the GDPR.<sup>25</sup>

In the run-up to this impact assessment, the Commission has been extensively consulting with all relevant stakeholders and in particular with the Member States. Thanks to the

---

<sup>17</sup> Major providers had to mitigate massive DDoS attacks: e.g. the attack against Amazon Web services in February 2020, with a peak traffic volume of 2.3 terabytes per second.

<sup>18</sup> COM(2020) 66 final.

<sup>19</sup> COM(2020) 605 final, 24 July 2020.

<sup>20</sup> Council 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.

<sup>21</sup> Commission Implementing Regulation (EU) 2019/1583.

<sup>22</sup> Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020) 595 final.

<sup>23</sup> For a discussion on the overlaps and differences between the NIS Directive and the GDPR, see ENISA (2019): Stock taking of security requirements set by different legal frameworks on OES and DSPs (<https://www.enisa.europa.eu/publications/stock-taking-of-security-requirements-set-by-different-legal-frameworks-on-oes-and-dsps>)

<sup>24</sup> 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.

<sup>25</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Cooperation Group, the Commission has been in constant touch with the competent authorities in charge of implementing the NIS Directive. The Cooperation Group has extensively covered various cross-cutting and sectoral implementation aspects. In addition, during its NIS country visits in 2019 and 2020, the Commission has interviewed 154 public and private entities, as well as 117 competent authorities. Member States and other stakeholders were also invited to participate in the Open Public Consultation and in the surveys and workshops organised by the NIS review study<sup>26</sup> on behalf of the Commission. Both the Open Public Consultation and the surveys explicitly also covered those entities that are currently not under the scope of the NIS Directive. The Commission has also published an inception impact assessment, to which stakeholders could submit feedback. *See also Annex 2 on stakeholder consultation.*

Being an initiative within the Regulatory Fitness Programme (REFIT), the impact assessment will not only look at ways to improve the cyber resilience of the Union but it will also examine to what extent the regulatory burden for competent authorities and compliance costs for public and private entities can be reduced.

## 1.2. Results of the evaluation of the NIS Directive

An evaluation on the functioning of the NIS Directive (*see Annex 5*) was conducted as part of the review process required by Article 23(2) of the NIS Directive. The conclusions of the evaluation can be summarised into six main categories of findings (*see Figure 1*). These findings are further elaborated on in the problem definition described below, linked to the problem drivers (*see section 2*). They are regarded as underlying causes for the identified problems.

EVALUATION	Increased interconnectedness & interdependencies in sectors not covered	Scope not clearly determined by the Directive & unclear national competence over DSPs	Divergent security and reporting requirements	Ineffective supervision and enforcement	Uneven resources for competent authorities set aside by Member States	Limited information sharing between Member States
	Scope (sectors, services, firm size)	OES identification & DSP coverage	Security measures & incident reporting	Supervision & enforcement	Capabilities of competent authorities	European cooperation

**Figure 1: Overview of the outcome of the evaluation**

### Evaluation finding 1: Increased interconnectedness and interdependencies in sectors not covered

The evaluation suggests that the current scope of the NIS Directive is too limited in terms of the sectors covered. This is mainly due to: (i) increased digitisation in recent years and a higher degree of interconnectedness, (ii) the scope of the NIS Directive no longer reflecting all digitised sectors providing key services to the economy and society as a whole.<sup>27</sup> Critical infrastructure (such as airports or hospitals) and other economic operators are becoming increasingly interconnected and reliant on network and information systems. Attacks on such infrastructure can therefore trigger chain reactions

<sup>26</sup> Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665. Wavestone, CEPS and ICF. The study kicked off in April 2020 and should be finalized by January 2021. The final report of the study was not yet submitted at the time of the writing of this report.

<sup>27</sup> Even though the NIS Directive does allow Member States to respond to such developments by bringing additional types of entities under the scope of the national laws transposing the Directive, only 11 out of 27 Member States made use of this possibility. This concerned a very limited number of very specific services (such as data centres, insurance companies or heat producers).

and send ripples throughout the economy.<sup>28</sup> The availability, integrity and confidentiality of a specific essential service cannot be effectively protected through regulatory requirements imposed on the provider of that service alone since the functioning of that service is affected by the level of protection of other sectors or services.<sup>29</sup>

### **Evaluation finding 2: Scope not clearly determined by the NIS Directive and unclear national competence over digital service providers**

Public and private entities that belong to the seven sectors under the NIS scope, as described in *section 1.1.*, are not automatically required to put in place security measures and report incidents. Member States must first identify them as operators of essential services (so-called OES identification process). The evaluation has shown that national authorities have developed a wide variety of identification practices leading to inconsistencies in the *de-facto* scope of the NIS Directive in the Member States. While this reflects the different approaches of Member States in determining the criticality of economic operators, it has led to a situation in which certain types of entities have not been identified in all Member States and are therefore not required to put in place security measures and report incidents.<sup>30</sup> The evaluation also identified that Member States are not fully aware of their potential competence for specific DSPs.

### **Evaluation finding 3: Divergent security and reporting requirements**

The NIS Directive allowed wide discretion to the Member States when laying down security and incident reporting requirements for OESs. The evaluation shows that in some instances Member States have implemented these requirements in significantly different ways. For example, Member States have modelled their national security requirements along different international standards or have chosen different degrees of prescriptiveness.<sup>31</sup> Incident reporting requirements also diverge considerably when it comes to *which* incidents need to be reported and *when and how* reports are to be made.

### **Evaluation finding 4: Ineffective supervision and enforcement**

For the purpose of supervision, competent authorities can request documentation from OESs, gather evidence of effective implementation of security policies and issue binding instructions to remedy deficiencies (so-called *ex-ante* supervision of OESs). During the country visits conducted in 2019-2020, the Commission observed that many Member States only make limited use of these options. In even fewer cases, they are systematically checking whether companies are complying with the NIS rules. The evaluation has also shown that the *ex-post* supervision approach<sup>32</sup> was not effective as far as the DSPs are concerned. This is notably due to: (i) the lack of a conclusive overview by the competent authorities of these services across the Member States, (ii) the lack of clarity of the jurisdiction rules and (iii) an insufficiently harmonised supervision and ineffective enforcement system. Finally, the evaluation has revealed that penalties are

---

<sup>28</sup> David Alexander (2008): A magnitude scale for cascading disasters. *International Journal of Disaster Risk Reduction*, Volume 30, Part B, September 2018, Pages 180-185.

<sup>29</sup> Tyson Macaulay (2019), *The Danger of Critical Infrastructure Interdependency*, <https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency>

<sup>30</sup> For example, five Member States have not identified any or only one OES in the health sector. At least eight Member States have not identified any OESs in the road transport subsector. At least four Member States have not identified any OESs in the railway subsector.

<sup>31</sup> These approaches range from very general provisions to very specific measures, such as specifying the minimum length of passwords.

<sup>32</sup> The *ex-post* supervision approach allows competent authorities to take supervisory measures only when provided with evidence that a DSP does not meet the security or notification requirements.

almost never applied and that there are considerable discrepancies when setting penalties across Member States, with the maximum level of penalties varying greatly.

### Evaluation finding 5: Uneven resources for competent authorities

The NIS Directive requires Member States to designate one or more competent authorities to supervise the implementation of the provisions thereof. In addition, Member States are required to designate a single point of contact (SPOC) for cross-border cooperation and one or more computer security incident response teams (CSIRTs) for incident handling. Despite the fact that the NIS Directive lays down detailed tasks for each of these authorities, the financial and human resources set aside by Member States for fulfilling these tasks, and consequently the different levels of maturity in dealing with cybersecurity risks, vary greatly. This makes it challenging for certain competent authorities to effectively meet their obligations stemming from the NIS Directive.

### Evaluation finding 6: Limited information sharing between Member States

Even though the current structures allowed for a substantial improvement in building mutual trust, Member States do not share information systematically with one another. In addition, there are deficiencies when it comes to the sharing of information between authorities within Member States. At EU level, the NIS Directive has created two new fora for information exchange between the Member States: the Cooperation Group to support and facilitate strategic exchanges and policy coordination, and the CSIRTs network, which promotes technical cooperation between national CSIRTs. Nonetheless, the exchange of information throughout the cybersecurity lifecycle remains limited and mostly unstructured. This is also the case for information sharing among private entities, and for the engagement between the EU level cooperation structures and private entities.

## 2. PROBLEM DEFINITION

### 2.1. What are the problems?

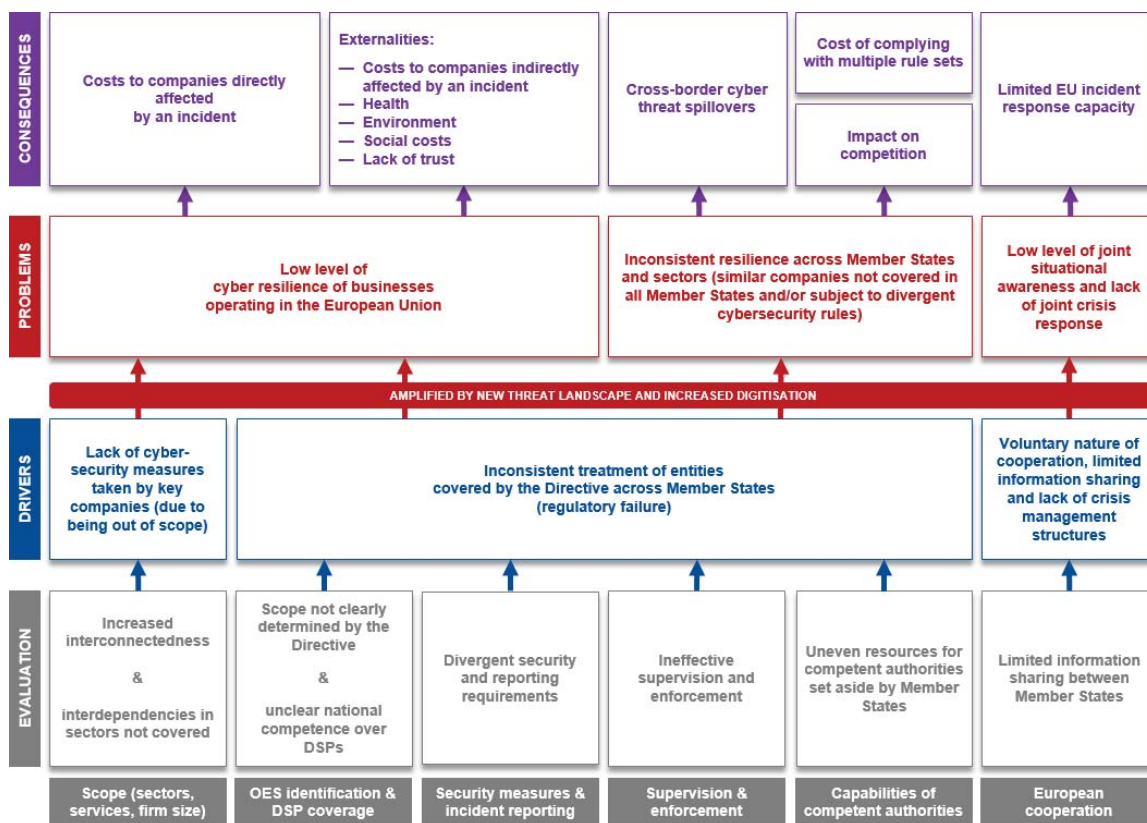


Figure 2: Outcome of the evaluation, problem drivers, problems and consequences



### 2.1.1. Low level of cyber resilience of businesses operating in the European Union

Cybercrime and cybersecurity can hardly be separated in an interconnected environment. Deterring cybercrime is an integral component of cybersecurity policies. Cybercrime comes at a high cost for societies and economies. A study of the Commission's Joint Research Centre (JRC)<sup>33</sup> stressed that **cybercrime is estimated to cost the world EUR 5.5 trillion by the end of 2020**, up from EUR 2.7 trillion in 2015, due in part to the exploitation of the COVID-19 pandemic by cyber criminals. According to the report: *'this figure represents the largest transfer of economic wealth in history, more profitable than the global trade in all major illegal drugs combined, putting at risk incentives for innovation and investment.'* The same study mentions that *'the number of citizens impacted simultaneously by a single cyber incident can be huge as a consequence of the pervasiveness of connected devices: 3 billion accounts in the attack on Yahoo in 2013, 77 million users in the attack on Sony PS3 in 2011, 1.3 million and 250 000 impacted citizens, respectively, in the attacks on Estonia and Ukraine in 2017, and 7 major security incidents in December 2019 alone. [...] In April 2007, Estonia [...] suffered a series of coordinated cyber attacks that targeted governmental institutions and bodies, financial entities, telecommunication infrastructure and newspapers. [...]*<sup>34</sup> The 2020 Digital Economy and Society Index (DESI)<sup>35</sup> shows that in 2020, 39 % of EU citizens who used the internet experienced security-related problems. In 2019, security concerns limited or prevented 50 % of EU internet users from performing online activities.

The JRC report stresses that the number of cyber-attacks has grown constantly over the years, with a corresponding growth in the resulting financial damage. The number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources inside and outside the EU. Microsoft's Digital Defence Report<sup>36</sup> confirmed that *'threat actors rapidly increased in sophistication in the past year, using techniques that make them harder to spot that threaten even the savviest targets.'*<sup>37</sup> In 2019, one in eight businesses were affected by cyberattacks<sup>38</sup>.

One cyber-attack alone can cause substantial damages across organisations, sectors, as well as citizens. The economic impact of the 2017 WannaCry incident is estimated in the order of hundreds of million euros with some cyber risk modelling analysts placing the losses in the order of billions. Apart from the economic costs, cyber-attacks can seriously affect and potentially lose lives. For example, in September 2020, a ransomware attack targeted a hospital in Düsseldorf; a death occurred after a patient who needed urgent care was diverted to a nearby hospital.<sup>39</sup>

---

<sup>33</sup> *Cybersecurity – Our Digital Anchor, a European perspective*, published in July 2020, page 7.

<sup>34</sup> *Idem*, page 9.

<sup>35</sup> <https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020>

<sup>36</sup> <https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/>, published in September 2020.

<sup>37</sup> The report also finds that *'criminal groups targeting businesses have moved their infrastructure to the cloud to hide among legitimate services [...]*' IoT threats were found in continuous expansion, pointing to an approximate increase of 35 % in total attack volume in the first half of 2020 as compared to the second half of 2019.

<sup>38</sup> According to Eurostat, 1 in 8 enterprises affected by ICT related security incidents (*Press release 'ICT security measures taken by vast majority of enterprises in the EU', 6/2020 - 13 January 2020*); as framed by the World Economic Forum 'Cyberattacks on critical infrastructure have become the new normal across sectors such as energy, healthcare, and transportation WEF, The Global Risks Report 2020.

<sup>39</sup> The case is currently being investigated by German authorities: <https://www.zdnet.com/google-amp/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/>

Cyber incidents do not only represent costs for those organisations directly affected by them (such as the entity where a breach has occurred or that has been the direct target of an attack) but they can also have an impact on the wider economy and society as a whole, including across borders<sup>40</sup>. For example, incidents can also cause costs to companies that have a link with the direct victim of an incident (for example, because the companies collaborate closely or because one company supplies goods or services to the other company<sup>41</sup>). Moreover, incidents can also have an impact on other parts of society (such as consumers or health care patients) and erode the trust in those entities that provide essential services.

A study looking at the cyber readiness of companies shows that most companies still have a long way to go. Even though there has been a marked increase in the proportion of businesses considered to be well prepared, 64 % are still considered to be novice in the field of cybersecurity.<sup>42</sup> Even for those (sub)sectors already covered by the NIS Directive, the results of the Open Public Consultation (OPC)<sup>43</sup> have shown that on average the level of cybersecurity resilience is assessed by respondents only as medium.<sup>44</sup> Regarding DSPs, respondents to the OPC consider them to exhibit a medium to high level of cyber resilience, with cloud services being regarded as the most resilient.<sup>45</sup> Small and medium sized enterprises (SMEs) in particular exhibit a relatively low level of cyber resilience.<sup>46</sup> At the same time, an overwhelming majority of 97 % of the OPC respondents indicated that the cyber threat level has increased since 2016.<sup>47</sup>

At the level of individual businesses, the 2020 Annual Cost of a Data Breach Report of the Ponemon Institute estimated the *average cost of a data breach* to be **EUR 3.5 million in 2018**, an increase of 6.4 % over the previous year<sup>48</sup>.

---

<sup>40</sup> Certain sectors exhibit a stronger cross-border dimension than other sectors. Especially energy, transport, banking, financial markets, digital infrastructures and digital services exhibit a particularly strong cross-border dimension.

<sup>41</sup> For example, supply chain company Resilience360 has recorded a total of 290 cyber security incidents in 2019 that had an impact on entities along the supply chain. See Resilience360 (2020): Annual Risk Report 2020 (<https://www.resilience360.dhl.com/resilienceinsights/resilience360-2020-annual-risk-report>).

<sup>42</sup> Hiscox Cyber Readiness Report 2020: [https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox\\_Cyber\\_Readiness\\_Report\\_2020\\_UK.PDF](https://www.hiscox.co.uk/sites/uk/files/documents/2020-06/Hiscox_Cyber_Readiness_Report_2020_UK.PDF). The study looks at companies in the United States, the United Kingdom and six EU Member States. In its cyber readiness model, the study classifies companies into one of three categories of cybersecurity preparedness: novice, intermediate, expert.

<sup>43</sup> Open Public Consultation on the revision of the NIS Directive. The survey was open from 7 July until 2 October 2020. All stakeholders were asked the same questions. However, some questions were more geared to certain stakeholder groups. As a result, stakeholders sometimes chose not to respond to certain questions. The OPC results in sections 2.1.1 and 2.1.2 only reflect the percentages of those stakeholders that did respond to a specific question.

<sup>44</sup> Respondents indicated that banking and financial market infrastructures exhibit a high level of cybersecurity resilience. They found the level of preparedness of the transport, health and drinking water sectors to be the lowest (but still within “medium”).

<sup>45</sup> The respondents to the OPC rate the level of preparedness of European SMEs with an average of 2.17 out of 5. Respondents from DSPs gave significantly higher ratings than other respondents regarding the preparedness of digital services.

<sup>46</sup> The highest ratings were given by trade associations and DSPs (2.3 each).

<sup>47</sup> Across all stakeholder groups there is a strong consensus that the cyber threat level has increased since 2016, including amongst stakeholders representing entities so far not covered by the scope. OESs and DSPs as well as cybersecurity professionals more frequently indicated that the cyber threat level has increased significantly.

<sup>48</sup> Annual Cost of a Data Breach Report, 2020, conducted by the Ponemon Institute, and based on quantitative analysis of 524 recent breaches across 17 geographies and 17 industries:

Member States have made significant progress when it comes to the cyber resilience of companies, notably by identifying thousands of entities across the Union and by requiring them to take cybersecurity measures and report incidents. Nonetheless, the level of cyber resilience in the Union remains relatively low. For example, when it comes to the level of cyber resilience in Europe in the global context, a study comparing the cyber resilience of companies across five world regions puts European companies behind Asia and America in all six areas that the study had focussed on.<sup>49</sup> In a recent comparative analysis of the cybersecurity programmes of companies in 18 major economies, EU companies scored significantly lower than their counterparts in the United States, South Korea and Japan.<sup>50</sup> Overall, this suggests that European businesses are not sufficiently prepared for cyber-related risks as compared to a global context.

At the same time, the cybersecurity landscape has changed considerably since the NIS Directive has come into force. The continuous digitisation is leading to an ever increasing attack surface. For example, more and more manufacturers are connecting industrial control systems (ICS) to the internet, with a year-on-year increase of connected ICS of 27 % between 2017 and 2018.<sup>51</sup> New technological trends also have an impact on the criticality of certain service providers so far not covered by the NIS Directive. For instance, content delivery networks (CDNs) have become a major part of the infrastructure of the modern internet. Since the NIS Directive has come into force in 2016, CDN-based internet traffic has overtaken non-CDN-based traffic and is projected to make up 72 % of total internet traffic by 2022.<sup>52</sup> The COVID-19 crisis and its impact on digitisation is expected to reinforce these trends even more. On the cybercrime side, attacks are increasingly becoming a commodity and can now often be achieved at very low costs. See Figure 3 from the JRC report with a screenshot taken from the dark web where various cyberattack ‘offers’ are advertised at very low prices.

OUR PRICING				
<b>1 Month Basic</b>	<b>Bronze Lifetime</b>	<b>Gold Lifetime</b>	<b>Green Lifetime</b>	<b>Business Lifetime</b>
<b>5.00 €</b> /month	<b>22.00 €</b> Lifetime	<b>50.00 €</b> Lifetime	<b>60.00 €</b> Lifetime	<b>90.00 €</b> Lifetime
1 Concurrent	1 Concurrent	1 Concurrent	1 Concurrent	1 Concurrent
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125 Gbps total network capacity	125 Gbps total network capacity	125 Gbps total network capacity	125 Gbps total network capacity	125 Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated support	24/7 Dedicated support	24/7 Dedicated support	24/7 Dedicated support	24/7 Dedicated support
<b>Order now</b>	<b>Order now</b>	<b>Order now</b>	<b>Order now</b>	<b>Order now</b>

<https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>

<sup>49</sup> PwC (2018): The Global State of Information Security 2018.

<sup>50</sup> ESI Thoughtlab (2018): The Cybersecurity Imperative ([https://www.protiviti.com/sites/default/files/United\\_States/insights/cybersecurity\\_imperative\\_2018.pdf](https://www.protiviti.com/sites/default/files/United_States/insights/cybersecurity_imperative_2018.pdf))

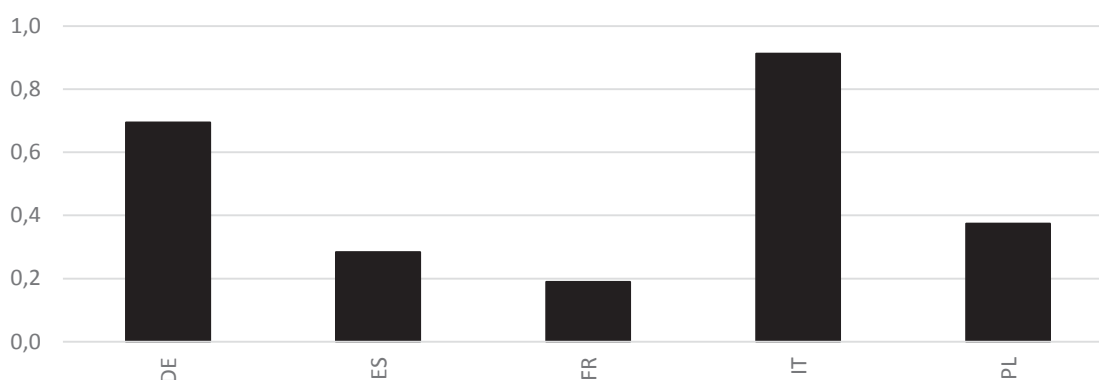
<sup>51</sup> Positive Technologies (2018): ICS vulnerabilities: 2018 in review (<https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/>)  
<https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/>

<sup>52</sup> Cisco (2019): Cisco Visual Networking Index: Forecast and Trends, 2017–2022

**Figure 3: Price list of a service offering DDoS attacks**<sup>53</sup>

### 2.1.2. Inconsistent resilience across Member States and sectors

The evaluation has shown that the NIS Directive has been a trigger for a significant EU-wide cybersecurity risk assessment undertaken by the Member States in those sectors covered by the Directive. As a result, competent authorities have identified thousands of public and private entities<sup>54</sup> as OESs, requiring them to take cybersecurity measures and report incidents. However, the evaluation has also revealed certain discrepancies in how Member States have transposed and implemented the rules of the NIS Directive. Entities can be subject to different regulatory treatment, depending on the jurisdiction that applies. This is especially true when it comes to the identification of OESs (i.e. whether entities are inside or outside the *de-facto* scope of the NIS Directive). For example, as shown in Figure 4, certain Member States (e.g. Italy) have identified much more OESs than other Member States (e.g. Spain, France).



**Figure 4: Number of identified OESs in the five biggest Member States (per 100,000 inhabitants)**

First and foremost, these discrepancies result in an uneven level of cyber resilience across the Union including among sectors, with entities sometimes not achieving the level of cyber resilience that the NIS Directive set out to achieve. Secondly, in the event of an incident, companies with a lower level of resilience can negatively impact even those companies that already exhibit a high level of resilience, as cyber threats and the costs of incidents can spread across supply chains and throughout the economy.<sup>55</sup> A recent Commission report (hereinafter called ‘the OES Report’) also highlights that due to the many interdependencies between companies in the internal market, discrepancies in OES identification can have serious consequences, including uneven degrees of cyber resilience that can lead to threats propagating more easily across borders.<sup>56</sup> It is the very nature of cybersecurity in the value chain that investments undertaken by one company

<sup>53</sup> JRC (2020): Cybersecurity – Our Digital Anchor, a European perspective: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor>

<sup>54</sup> Overall, Member States have reported 15,676 identified OESs to the Commission, 10,897 of which were identified by Finland.

<sup>55</sup> Tyson Macaulay has published a Dependency Matrix for 10 Critical Infrastructure Sectors, which highlights the importance of a consistently high level of cyber resilience across the economy. See Tyson Macaulay (2019): The Danger of Critical Infrastructure Interdependency, <https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency>.

<sup>56</sup> Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems. COM(2019) 546 final.

can have a positive impact on the cybersecurity of other companies (externalities).<sup>57</sup> In the OPC, 97 % of respondents agreed that “*cyber risks can propagate across borders at high speed, which is why cybersecurity rules should be aligned at Union level*”.<sup>58</sup> An inconsistent resilience across Member States can therefore contribute to the negative consequences for the economy and society that *section 2.1.1* describes in detail.

In the OPC, 80 % of stakeholders disagreed with the statement that “*there is a sufficient degree of alignment of security requirements for OES and DSPs in all Member States*”.<sup>59</sup> Similarly, when asked about notification requirements, 60 % of stakeholders disagreed with the statement that the “*current approach ensures that OES across the Union face sufficiently similar incident notification requirements*”.<sup>60</sup>

There are also notable differences in the level of cyber resilience across different NIS sectors: In the OPC, respondents were asked to evaluate the level of cyber resilience of the different sectors and digital services covered by the NIS Directive on a scale from “very low” to “very high”. Sectors such as banking, financial market infrastructure and digital infrastructure are considered as much more resilient than the other sectors with health, transport and drinking water supply scoring particularly low. These results are very much in line with the conclusions drawn by the Commission after the NIS review country visits.<sup>61</sup> According to a recent report of the Ponemon Institute on the cost of data breaches<sup>62</sup>, the healthcare sector, for the tenth year in a row, continued to incur the highest average breach costs at global level, at about EUR 6.13 million: a 10 % increase as compared to the previous year estimates. Similarly, the energy sector saw a 13 % increase from 2019, to an average of EUR 5.50 million. Overall, 13 of 17 industries experienced an average total cost decline year over year.

Discrepancies in the way entities are treated by the Member States not only have consequences on the level of cyber resilience, but can also have a meaningful impact on the internal market: Divergent requirements create an uneven level playing field for companies that are active across the internal market, putting providers of essential services in certain Member States at a disadvantage compared with similar providers in other Member States. 69 % of OPC respondents disagree with the statement that the “*identification process has contributed to the creation of a level playing field for companies from the same sector across the Member States*”.<sup>63</sup> Respondents to the Commission’s inception impact assessment are also very critical of the OES

---

<sup>57</sup> IPACSO: A Coordination Action under the FP7 DG CNECT Trustworthy ICT Program, deliverable D4.1

<sup>58</sup> Most respondents not only agreed but even strongly agreed with this statement. Respondents throughout all stakeholder groups tended to agree with the statement, including respondents representing entities from sectors so far not covered. The smallest percentage of respondents agreeing with the statement was found amongst competent authorities, of which “only” 83 % agreed with the statement.

<sup>59</sup> Respondents throughout all stakeholder groups (including respondents representing entities from sectors so far not covered) tended to disagree with the statement with the exception of competent authorities of which only 50 % disagreed.

<sup>60</sup> Only 50 % of competent authorities disagreed with the statement. However, 57 % of the OESs and 78 % of trade associations disagreed, including a majority of respondents representing entities from sectors so far not covered.

<sup>61</sup> Conducted by the Commission as part of the NIS review process in 2019-2020.

<sup>62</sup> Annual Cost of a Data Breach Report, 2020, conducted by the Ponemon Institute, and based on quantitative analysis of 524 recent breaches across 17 geographies and 17 industries: <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>

<sup>63</sup> However, only 57 % of competent authorities disagreed with this statement and 53 % of cybersecurity professionals actually agreed with it. 60 % of OESs and 90 % of trade associations disagreed.

identification process, citing the lack of alignment as a major problem. Respondents have commented that the current approach can have negative consequences for competition, as similar companies might be subject to different requirements depending on the Member State where they operate.

Moreover, having to cope with a multitude of requirements can increase the regulatory burden and costs for companies active in several Member States. 94 % of OPC respondents agree with the statement that from an internal market perspective the general *“approach [of the Directive] increases costs for OES operating in more than one Member State”*.<sup>64</sup> When it comes to security requirements, 93 % of the OPC respondents agree with the statement that the *“different level of prescriptiveness of requirements increases the regulatory burden for companies operating across different national markets”*.<sup>65</sup> Regarding incident reporting requirements, 87 % of respondents feel that the *“different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES”*.<sup>66</sup> The many different reporting requirements a company is facing across the internal market do not only increase its costs but can also consume valuable resources that could be used for the handling of an incident. Along similar lines, the respondents to the Commission’s inception impact assessment are largely in favour of more harmonized security and incident notification requirements.

When it comes to national enforcement, 75 % of respondents that provided an answer disagreed with the statement that *“there is a sufficient degree of alignment of penalty levels between the Member States”*.<sup>67</sup> Finally, 86 % of respondents support the statement that the approach of the Directive *“leads to significant differences in the application of the directive and has a strong negative impact on the level playing field for companies in the internal market”*.<sup>68</sup>

### 2.1.3. Low level of joint situational awareness and lack of joint crisis response

The cooperation between Member States in the field of cybersecurity does not lead to joint situational awareness from a strategic and operational point of view. Strategically, national authorities do not gather or share information to assess the state of cybersecurity in the EU nor structured feedback from businesses. Operationally, there is no regular information sharing on the impact of cybersecurity incidents and threats at national or EU level.

The sharing of information about incidents within the Cooperation Group is voluntary and on ad-hoc basis<sup>69</sup>. As a result of the small number of incidents reported on national level (*section 2.2.1*), the incidents submitted annually by Member States to the Cooperation Group<sup>70</sup> only represent a small subset of the incidents taking place within

---

<sup>64</sup> The statement is supported by almost all stakeholder categories, including respondents representing entities from sectors so far not covered. However, 60 % of competent authorities disagreed.

<sup>65</sup> The statement is supported by stakeholders throughout all categories.

<sup>66</sup> However, only 63 % of competent authorities agreed with this statement.

<sup>67</sup> Stakeholders throughout all categories disagreed with this statement. Cybersecurity professionals tended to disagree the least, with “only” 64 % disagreeing with the statement.

<sup>68</sup> This statement was controversial despite the fact that it is supported by a large majority: Almost all stakeholder groups support the statement, with DSPs and trade associations supporting it the most strongly with 100 % and 92 % respectively. However, all competent authorities disagreed with it.

<sup>69</sup> With the exception of the annual summary report to the Cooperation Group on the notifications received (Article 10(3) of the Directive).

<sup>70</sup> See Article 10(3) of the NIS Directive.

the EU. Member States have rarely made use of the cross-border notification provisions<sup>71</sup>, which require them to inform other Member States affected by incidents.

Despite the efforts of the Cooperation Group, the information exchange between Member States on cross-border dependencies remains limited, leading to conclude that Member States are not fully integrating potential cybersecurity-related cross-border spillovers into their risk assessments.

As far as the CSIRTs network is concerned, information is shared also on an ad-hoc basis and does not contribute to the development of a systematic, comprehensive situational picture about incidents identified across the EU.<sup>72</sup>

Under the current rules, neither the Commission nor the cooperation fora are able to:

- systematically analyse and detect differences and patterns in attack intensity between Member States and sectors, subsectors and types of entities,
- jointly determine in which (sub)sectors and types of entities competent authorities should channel resources,
- have a comparative view across Member States on the resilience and preparedness of public and private entities and the degree of institutional maturity.

Finally, there is no mutual assistance in incident response (operational cooperation)<sup>73</sup> on European level beyond the sharing of information within the different cooperation fora established by the NIS Directive.<sup>74</sup> For example, Member States do not lend operational support to each other in the event of a major incident or crisis, including during the recent COVID-19 crisis, which gave rise to a number of new cybersecurity related challenges.<sup>75</sup>

## **2.2. What are the problem drivers?**

### *2.2.1. Lack of cybersecurity measures taken by key companies*

Overall, only a limited number of sectors is covered by the NIS Directive and, within these sectors, there are inconsistencies in the OES identification. As a result, a significant number of companies providing essential services outside the scope of the NIS Directive but also some companies in the sectors listed by the NIS Directive are not required by law to put in place adequate cybersecurity measures and report incidents. This includes new economic activities which have only relatively recently taken on an essential role within the economy, such as social networks. The fact that several Member States chose to apply the NIS Directive to additional sectors further highlights that the current scope

---

<sup>71</sup> Article 14(5) and 16(6) of the NIS Directive.

<sup>72</sup> To improve the flow of information and enhance operational cooperation, the CSIRTs network is developing joint communication means, notably the MeliCERTes platform connecting national CSIRTs.

<sup>73</sup> Mutual assistance is mentioned among the tasks of the CSIRTs network in Article 12(3)(e) but only for cross-border incidents and on a strictly voluntary basis. As a result, it does not take place in practice.

<sup>74</sup> It is worth noting that with the publication of the Blueprint in 2017, the Commission launched a first non-binding initiative to coordinate the response to large scale cybersecurity incidents and crises. As a result, Member States have developed at operational level the Cyber Crisis Liaison Organisation Network (CyCLONe) Network which is not yet operational. CyCLONe was launched during the Blue OLEx 2020 exercise on 29 September 2020 and constitutes the operational layer of the Blueprint. It is a forum where Member State representatives meet to discuss aspects of operational cooperation in the event of a cybersecurity crisis.

<sup>75</sup> Such as a marked increase in the use of virtual private networks and video conferencing tools.

of the Directive does not reflect all the entities considered as essential in a highly digitised and interconnected economy.<sup>76</sup>

The scope of the NIS Directive covers certain types of entities in seven sectors (OESs) and, in addition, three types of DSPs. The Statistical Classification of Economic Activities in the European Community (NACE) groups economic activity into 21 economic areas. Only six of these economic areas are covered by the Directive and within each of these areas only a subset of types of entities are included in the scope. The scope of the NIS Directive therefore only represents a fraction of the economic activities in the Member States.

Investment in cybersecurity by entities not falling under the scope of the NIS Directive remains limited because entities do not have to bear the full costs of a potential incident, as some of the costs have to be borne by other parties, such as suppliers or customers. These negative externalities<sup>77</sup> create an incentive for businesses not to limit their exposure to risk (so-called moral hazard).<sup>78</sup> In addition, since in an interconnected economy the security of one institution highly depends on the security of other institutions (so-called interdependent security), companies have an incentive to free-ride by profiting from the security measures taken by other companies without sufficiently investing in cybersecurity themselves.<sup>79</sup> Recent survey data suggests that moral hazard does play a role in investment decisions, with companies citing regulatory compliance as the leading factor for cybersecurity spending and not cybersecurity-related factors, such as reducing incidents and breaches.<sup>80</sup>

## 2.2.2. *Inconsistent treatment of entities covered by the Directive across Member States*

### *Underlying driver 1: Discrepancies in OES identification and DSP coverage*

In the OES report, the Commission has shown that there is a certain degree of fragmentation across the Union as regards the identification of OESs. National authorities have developed a wide variety of identification practices when it comes to the overall approach to OES identification, but also regarding the definition of essential services.<sup>81</sup> For example, in the electricity subsector some Member States have identified “electricity supply” as an essential service while others have broken that service down into very granular categories, such as “distribution”, “transmission” or “production”. Moreover, there are inconsistencies between the thresholds used by competent authorities to identify OESs. For example, in the drinking water supply and distribution sector, some Member States identify waterworks as OESs when they serve more than 10,000 consumers while other Member States have set an OES identification threshold of 500,000 consumers. In addition, thresholds do not only vary quantitatively<sup>82</sup> but also

---

<sup>76</sup> For example, 5 Member States have identified additional information infrastructures, such as data centres. Another 4 Member States have identified government services, such as electronic services for citizens. A more detailed list can be found in Annex 4.

<sup>77</sup> Haislip and Kolev (2019): The economic cost of cybersecurity breaches: A broad-based analysis: <https://pdfs.semanticscholar.org/6630/44a95466583951c77df23389d25c1fef5db0.pdf>

<sup>78</sup> Vagle (2020): Cybersecurity and Moral Hazard. Stanford Technology Law Review, Vol. 23:1, p. 71.

<sup>79</sup> Tyler Moore (2010): The Economics of Cybersecurity: Principles and Policy Options, International Journal of Critical Infrastructure Protection, Volume 3, Issues 3-4, December 2010, Pages 103-117.

<sup>80</sup> Barbara Filkins (2020) “Spends and Trends: SANS 2020 IT Cybersecurity Spending Survey”, SANS Institute: Information Security Reading Room, 450 respondents.

<sup>81</sup> The Directive allows Member States to apply sector-specific thresholds in addition to cross-sectoral ones. This can give rise to a very complex mix of thresholds and has a negative impact on overall OES identification consistency.

<sup>82</sup> For example, some Member States identify authoritative DNS servers responsible for handling more than 50.000 domain names as OESs while others have set the thresholds to 100.000 domain names.



qualitatively<sup>83</sup>. This diversity is partly due to the design of the NIS Directive (which provides Member States with a considerable level of discretion) and partly due to the different implementation methodologies used by the Member States. Because of the current identification landscape, the scope of the NIS Directive becomes fragmented, with some operators subject to additional regulation (because they have been identified by their respective Member State) while others providing similar services remaining excluded and not having to put in place cybersecurity measures (because they have not been identified).

The identification of critical entities has traditionally been a central element of critical infrastructure protection. It has the clear benefit of taking into account regional or national specificities. And while identification can be considered a reasonable approach for ensuring resilience of critical infrastructure against non-cyber threats, the diversity produced by the identification process laid down in the NIS Directive seems inappropriate for raising the level of resilience of entities when it comes to cybersecurity, especially given their high degree of interconnectedness, the increased digitisation of the economy and the many interdependencies between operators and sectors.

Competent authorities also reported major shortcomings in the design of the NIS Directive regarding the extent to which DSPs are covered by national rules. DSPs located in the EU fall under the jurisdiction of the Member State where they have their main establishment.<sup>84</sup> However, the NIS Directive does not provide enough guidance to determine the main establishment. The non-EU based DSPs which offer services within the EU are deemed under the jurisdiction of the Member State where they have designated a representative. However, the NIS Directive does not require DSPs to inform the competent authority of the very Member State in which they have designated their representative. Taking into account the specific nature of digital services<sup>85</sup>, the NIS Directive does not provide competent authorities with the necessary powers and means to determine which entities fulfil the requirements for being subject to their own jurisdiction and which fall under the jurisdiction of other Member States. As a result, competent authorities cannot exercise effectively their supervision tasks, with the consequence that DSPs are often *de facto* excluded from the application of the directive's rules.

#### *Underlying driver 2: Inconsistent security measures and reporting requirements*

The NIS Directive grants Member States considerable discretion to define both the cybersecurity measures that OESs have to put in place and the procedures and thresholds for reporting incidents. As a result, entities are faced with a wide range of different approaches across the Union.

The evaluation of the functioning of the NIS Directive identified several inconsistencies in how security requirements have been put in place. For example, while most Member States have modelled their national requirements in line with international standards, some have chosen different standards (such as the ISO 27000-series or NIST standards) or even more specific national provisions. Member States have also chosen different degrees of prescriptiveness for the requirements. While some Member States imitated the approach of the NIS Directive by putting forward very general provisions, others are requiring companies to take very specific measures, which can go as far as specifying the minimum length of passwords.

---

<sup>83</sup> For example, some Member States take into account the “number of connected autonomous systems” when identifying internet exchange points, while others rely on “market share” as relevant indicator.

<sup>84</sup> Article 18 of the NIS Directive.

<sup>85</sup> DSPs provide cross-border services, often without any direct link to the physical infrastructure in the Member States.

Along similar lines, Member States are free to define thresholds on *which* incidents to report. Even though Member States are required to take into account several factors (the number of users affected by an incident, its duration and its geographical spread), they are at liberty to set their own quantitative thresholds. As a result, the number of incidents reported by OESs in each Member State differs significantly and does not reflect the scale of incidents affecting companies' network and information systems: For example, during the 2019 annual summary reporting exercise, while one Member State reported to have received 266 incident reports, six Member States have received either no or only one single incident report. The remaining Member States received between 2 and 31 reports. Overall, Member States have defined relatively high thresholds for incident reporting for OESs<sup>86</sup>, which has led to only few incidents being reported.

Member States are also free to determine *at what time and how* an incident shall be reported.<sup>87</sup> Companies operating in several Member States are therefore confronted with a variety of different reporting requirements.

### *Underlying driver 3: Ineffective supervision and enforcement*

While the NIS Directive requires Member States to ensure that competent authorities have the powers and means to assess operators' compliance of essential services with their obligations, it does not define any supervisory standards that competent authorities should live up to. As a result, the supervisory measures taken by competent authorities deviate significantly and put in question their effectiveness. For example, in-depth checks of the security measures taken by OESs are limited.

While the NIS Directive requires competent authorities to supervise OESs in an active manner, this is not the case for DSPs: Despite the fact that digital services covered by the Directive, such as cloud services, are just as essential for the economy as services provided by OESs<sup>88</sup>, DSPs are only to be supervised reactively *ex-post* (i.e. once the authority has been made aware of any shortcomings). This means that a large majority of DSPs in the internal market does not face any compliance checks at all. As a matter of fact, as most competent authorities are not even aware of the names of the DSPs falling under their jurisdiction, most DSPs are essentially never in touch with the authorities that are supposed to supervise them.

As regards enforcement, the NIS Directive neither provides for principles and/or types of sanctions Member States should provide for in their national legislation, nor does it guide Member States on penalty levels that could ensure effectiveness, proportionality and dissuasiveness. The evaluation of the functioning of the NIS Directive has shown that, as a result, penalty levels vary considerably between Member States. For example, the level of maximum penalties ranges from around EUR 1,400 to EUR 5,000,000<sup>89</sup>, or in the case of Member States applying percentages of the global annual turnover of undertakings, from 0.5% to 5%. With a median maximum penalty of around EUR 100,000, maximum penalties are too low in most Member States and are therefore neither effective nor dissuasive, especially when it comes to large companies. In addition, competent

---

<sup>86</sup> The same applies for DSP thresholds defined in the Commission Implementing Regulation (EU) 2018/151.

<sup>87</sup> This has resulted in a wide range of obligations, some Member States requiring a first incident report "as soon as possible" or 2 hours after the incident occurred, while others requiring it after 72 hours.

<sup>88</sup> The provision of essential services heavily depends on cloud services. Cloud services are therefore increasingly regarded as a backbone for the provision of other essential services.

<sup>89</sup> Some Member States are undergoing a legislative process to amend the cybersecurity framework, including in relation to the level of fines. For example, Germany included in a draft security law provisions on penalties up to 20.000.000 EUR or 4 % of the global annual turnover.

authorities have so far been reluctant to actually apply penalties.<sup>90</sup> Not a single case of a penalty having been applied to a public or private entity has been brought to the attention of the Commission at the time of writing of this report.

#### *Underlying driver 4: Discrepancies in Member State capabilities*

There are significant differences in capability amongst Member States when it comes to dealing with the challenges posed by cyber threats. In the National Cyber Security Index from 2018, which provides an overview of the cyber security capacity of 100 countries worldwide, EU Member States differ significantly, scoring between 31.17 and 83.12 (out of a maximum of 100 points).<sup>91</sup> Along similar lines, the Global Cybersecurity Index 2018 of the UN specialised agency for ICT (International Telecommunication Union – ITU) ranks EU Member States from 0.479 to 0.918 (on a scale from 0 to 1).<sup>92</sup> It is worth noting that Member States were still in the process of fully transposing the NIS Directive at the time of writing of the two above-mentioned indexes. In fact, the Commission’s country visits in 2019 and 2020 have revealed major progress across the Union when it comes to national capabilities. Nonetheless, the country visits have also shown that competent authorities still exhibit different degrees of maturity when it comes to primary NIS-related tasks, such as OES identification, incident handling, supervision and cross-border cooperation. The Commission has also observed major differences in the degrees of achievement of a well-functioning cybersecurity ecosystem, including the ability to offer technical support to operators or set up sectoral or cross-sector cooperation fora.

The amount of resources dedicated to cybersecurity policies at national levels and the degree of maturity in dealing with cybersecurity risks depend to a great extent on the level of economic development (different spending capacities), political prioritisation and advancement of cybersecurity measures prior to the NIS Directive. The impact of economic development is exacerbated by the fact that cybersecurity professionals compete on a European (if not global) market. During the NIS country visits, competent authorities from some Member States have lamented the fact that they do not have the financial capacities to compete with market salaries.

#### *2.2.3. Voluntary nature of cooperation, limited information sharing and lack of crisis management structures*

##### *Underlying driver 1: Voluntary nature of cooperation*

The provisions on cooperation laid down by the NIS Directive are often very general in nature. As a result, Member States tend to interpret them as voluntary. For example, the NIS Directive requires Member States to consult one another before identifying OESs that provide services in more than one Member State.<sup>93</sup> To support Member States in carrying out cross-border consultations, the Cooperation Group issued a reference document in July 2018.<sup>94</sup> However, only very few Member States have used the cross-border consultation procedure to engage with one another. Only two Member States have done so in a systematic manner.<sup>95</sup> The main reasons for this lack of engagement are the

---

<sup>90</sup> The Commission is aware of instances in which Article 21 of the NIS Directive would have allowed the Member States in question to apply penalties.

<sup>91</sup> National Cyber Security Index 2018, e-Governance Academy: [https://ega.ee/wp-content/uploads/2018/05/ncsi\\_digital\\_smaller.pdf](https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf)

<sup>92</sup> ITU Global Cybersecurity Index 2018: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf)

<sup>93</sup> Article 5(4) of the NIS Directive.

<sup>94</sup> Identification of Operators of Essential Services – Reference document on modalities of the consultation process in cases with cross-border impact, Cooperation Group Publication 07/2018.

<sup>95</sup> As shown by the OES report, COM(2019) 546 final.

fact that the NIS Directive does not specify how such consultations are supposed to be carried out or whether the authorities are required to mutually agree on a certain outcome of the consultation procedure. Also, no platform is provided to facilitate the exchange of confidential information between Member States (such as on cross-border dependencies).

Moreover, in the event of an incident affecting another Member State, competent authorities are obliged to inform the other affected Member State if the incident significantly affects the continuity of essential services in that Member State. However, the NIS Directive does neither specify the modalities for information sharing nor does it set common objectives incentivising such exchange. As a result, this kind of information exchange rarely takes place.

Finally, it is worth pointing out that the problems described in this section cannot be fully addressed by issuing additional guidance in the Cooperation Group alone, as Cooperation Group guidance is again voluntary and non-binding in nature, lacking the appropriate means to align national approaches to implementation.

#### *Underlying driver 2: Limited information feeding into the existing groups*

The Cooperation Group receives a summary report of incidents notified under the NIS Directive in each Member State, which represents a small subset of the overall incidents handled by an authority. The focus on incidents leaves out a wealth of information making it difficult to develop a shared understanding of the level of cybersecurity capabilities across the Union (e.g. uptake of cybersecurity solutions, human capital, level of skills in cybersecurity, maturity levels among sectors). Furthermore, the interaction with the private sector is limited and unstructured, making it difficult to reflect the needs of European stakeholders.

#### *Underlying driver 3: Lack of crisis management structures*

Cooperation under the NIS Directive is voluntary and does not cover the entire crisis management cycle (from preparedness to coordinated response). The mandates of the Cooperation Group and the CSIRTs network, two fora setup by the NIS Directive to facilitate information sharing, also do not include crisis management. The Blueprint recommendation<sup>96</sup>, adopted in 2017, was the first EU attempt to improve cooperation in times of crisis. However, while representing a valuable first building block, the recommendation remains non-binding and the task of building comprehensive EU crisis management framework remains incomplete.

### **3. HOW WILL THE PROBLEM EVOLVE?**

Emerging technologies will continue to drive digitisation within the economy and society as a whole. Increased use of artificial intelligence (AI), advancements in quantum computing or the roll-out of 5G networks are just some of the examples of how companies providing essential services will become even more reliant on technology and connectivity, resulting in an ever larger attack surface for malicious actors.

According to the Internet Security Forum, cybersecurity will remain a major concern in the coming years: *“By 2022, organisations will be plunged into crisis as ruthless attackers exploit weaknesses in immature technologies and take advantage of an unprepared workforce. [...] The impact of threats will be felt on an unprecedented scale*

---

<sup>96</sup> Commission Recommendation of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises, C(2017) 6100 final.

*as aging and neglected infrastructure is attacked and disrupted due to vulnerabilities in the underlying technology.*"<sup>97</sup>

As a result, **the number of cybersecurity incidents within the EU is likely to increase, triggering further costs** for the companies directly affected by these incidents but also for the wider economy and citizens, as threats spread along supply-chains.

As the general awareness of cyber-related risks is increasing, public and private entities in sectors outside the scope of the NIS Directive are likely to step up their investments in cybersecurity to some extent even without additional regulation.<sup>98</sup> Estimates based on Gartner forecasts suggest that even for the sectors already covered by the NIS Directive, the ICT security spending is projected to grow by 12 % in the coming three to four years (*section 7.1*). At the same time, innovation in the field of cybersecurity and the roll-out of technologies with the potential of raising the level of cyber resilience<sup>99</sup> will also contribute to making the provision of essential services more secure.

However, **in the absence of further regulatory intervention, moral hazard and the free-riding behaviour as described in section 2.1.1 will not disappear**, as companies lack the incentives necessary to take into account the broader societal cost of cyber incidents when determining their level of investment in cybersecurity. At the same time, digitisation and exposure to cyber risks across sectors will continue to mount. As a result, public and private entities are very unlikely to take all the measures necessary to achieve a high level of cyber resilience on a voluntary basis. This is especially true for those entities currently not covered by the provisions of the NIS Directive, such as manufacturing companies or data centres, but also for entities that are under the scope of the NIS Directive but whose level of cyber resilience remains low due to problems and drivers described in *sections 2.1.2* and *2.2.2* respectively.

As the **discrepancies in the OES identification process** are mainly caused by the way in which the NIS Directive has been designed, they are very unlikely to disappear without additional intervention. Nonetheless, the Cooperation Group may continue issuing non-binding guidance to further align the identification process. In addition, some Member States have notified the Commission that they intend to identify additional operators in the near future. As a result, some of the discrepancies observed may be reduced as the national implementation of the NIS Directive is becoming more mature, but nevertheless such **alignment is expected to be rather limited**.

As to the **regulatory coverage of DSPs** across the internal market, the provisions of the NIS Directive will continue to prevent competent authorities from ensuring that all companies take adequate cybersecurity measures.

The Cooperation Group will continue issuing non-binding guidance to further align security measures across the Member States. However, as described in the evaluation on the functioning of the NIS Directive and in *section 2.2.2*, Member States have chosen very different approaches to imposing security measures. It will therefore be very **difficult to encourage Member States to align measures** to such an extent that the negative effects of fragmentation will disappear.

---

<sup>97</sup> Internet Security Forum (2020): Threat Horizon 2022: Digital and physical worlds collide, <https://www.securityforum.org/research/threat-horizon-2022-digital-and-physical-worlds-collide/>.

<sup>98</sup> For example, according to the Gordon–Loeb model analyzing the optimal investment level in information security, companies have an intrinsic incentive to invest into cybersecurity to at least some extent based on the risk and potential costs of an incident.

<sup>99</sup> For example, the uptake of internet protocols, such as DNSSEC, which enhances the integrity of the domain name system (DNS) by introducing cryptographic authentication, can have a positive impact on the cybersecurity of internet infrastructure.

As regards supervision, it is likely that the wide differences among supervisory approaches taken by competent authorities at national levels will be maintained, influenced also by the overall level of cybersecurity maturity and resources available. Furthermore, because of the shortcomings of the NIS Directive described in *section 2.2.2*, it is **unlikely that all entities across the internal market will become subject to adequate supervisory measures**. As to the supervision of DSPs across the Union, the shortcomings of the NIS Directive, notably as regards the overview by the competent authorities, the applicable jurisdiction rules and the supervisory regime make it likely for these to continue to operate under the radar of competent authorities.

With the NIS ecosystem expected to become more mature in the coming years and the increased awareness of policy makers regarding cyber risks, it is possible that Member States will provide more funding to competent authorities. However, as the problem drivers described in *section 2.2.2* are of a long-term structural nature, the **discrepancies in Member State capabilities are likely to remain considerable**.

The regular exchange and cooperation within the fora established by the NIS Directive is likely to continue to have a positive effect on trust and confidence amongst their members and can further boost information sharing in the medium term. Nonetheless, as described in *section 2.2.2*, the lack of information exchange and the deficiencies in the existing structures facilitating stakeholder consultation and operational cooperation, including crisis management, will **continue to prevent a notable increase in information sharing and operational cooperation**.

#### **4. WHY SHOULD THE EU ACT?**

##### **4.1. Legal basis**

The current legal basis of the NIS Directive is Article 114 of the Treaty on the Functioning of the European Union (TFEU), whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. Any proposed actions would build on the objectives of the current NIS Directive. They would also improve the level playing field for companies in the internal market, subjecting them to the same requirements across the Union. Any new legislative act would therefore have the same legal basis as the current NIS Directive.

##### **4.2. Subsidiarity: Necessity of EU action**

Cybersecurity resilience across the Union cannot be effective if approached in a severed manner through national or regional silos. The NIS Directive came to address this shortcoming, by setting a framework for network and information systems security at national and Union levels for legal, policy, institutional, technical and operational measures, as well as for cross-border cooperation. The transposition and implementation of the NIS Directive also brought to light inherent flaws of certain provisions or approaches which, in spite of the intended effects, affected the authorities' and industries' focus on core cybersecurity issues. As described in *section 2* above, some of these flawed provisions concern the unclear delimitation of the scope of the NIS Directive leading to fundamental differences in the extent and depth of *de facto* EU intervention at Member State level. Furthermore, while notable progress was made in terms of cooperation across borders, the current voluntary cooperation remains largely at policy level, while at operational level it is rather limited to an ad-hoc or regional basis. All these inherent flaws have eventually led to considerable disparities across the Member States in terms of capabilities, planning and level of protection, which affect at the same time the level playing field for similar companies on the internal market.

Information asymmetry and lack of transparency risk undermining the supply by market operators and manufacturers of networks, services and products, as well as the trust of the users, which is one of the key drivers of the internal market.

Last, but not least, well-functioning networks and systems are essential for the EU economy. Since the COVID-19 crisis, the European economy has grown more dependent on network and information systems than ever before and sectors and services are increasingly interconnected. Disruptions resulting from cybersecurity incidents are increasing in frequency and magnitude with the potential of undermining the internal market, including negative consequences for growth and jobs.

For all the above-mentioned reasons, the first periodical review of the NIS Directive, as requested by Article 23 thereof, created the opportunity for further EU action in relation to the NIS framework. Such EU action would also aim at addressing more effectively cases with cross-border relevance, where further coordination at the level of planning and response, as well as mutual assistance, are needed.

#### **4.3. Subsidiarity: Added value of EU action**

EU intervention going beyond the current measures of the NIS Directive is justified by the subsidiarity principle mainly due to the:

- *cross-border nature of the problem.* Given the cross-border nature of NIS threats and problems, a non-intervention at EU level to improve the current NIS framework would lead to a situation where Member States' joint action would remain rather limited, taking insufficient account of the cross-border and cross-sector interdependence as regards the network and information systems. An appropriate degree of coordination among the Member States, on the other hand, would ensure that NIS-related risks can be well managed in the cross-border context in which they also arise, and therefore respects the subsidiarity principle.
- *potential of EU action to improve and facilitate effective national policies.*
- *contribution of concerted and collaborative NIS policy actions to effective protection of fundamental rights, specifically the right to the protection of personal data and privacy.* European citizens are increasingly entrusting their data to complex information systems, either out of choice or out of necessity, without necessarily being able to correctly assess the related data protection risks. When incidents occur, they will therefore not necessarily be able to take suitable steps, nor is it certain that the Member States would be able to effectively address cross-border incidents in the absence of an effective EU-wide NIS coordination.

As regards the *proportionality of the approach*, the measures in the policy options considered do not go beyond what is needed to achieve the general and specific objectives, and do not impose disproportionate costs. As shown in *sections 7 and 8*, the measures proposed in the considered policy options to further streamline the security requirements and reporting obligations at Union level take account of the already existing practices in the Member States. An enhanced level of protection achieved through such streamlined requirements would be proportionate to the risks faced and hence reasonable and generally corresponding to the interest of the entities involved in ensuring continuity and quality of their services. The costs for ensuring systematic cooperation amongst Member States would be small when compared to the economic and societal losses and damages which may be caused by NIS incidents. Furthermore, the stakeholder consultations held in the context of the NIS review, including the OPC results (*Annex 2*) and the targeted surveys conducted by the NIS review study (*Annex 6*) show support for the revision of the NIS Directive along the above-mentioned lines.

## 5. OBJECTIVES: WHAT IS TO BE ACHIEVED?

This section identifies the general and strategic objectives for a possible EU intervention to address the gaps identified in section 1.

### 5.1. General objectives

There are three general policy objectives, which describe the overarching goals of a possible EU intervention:

- 1) **Increase the level of cyber resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors**, the main general objective, by putting in place rules that ensure that all public and private entities across the internal market, which fulfil important functions for the economy and society as a whole, are required to take adequate cybersecurity measures.
- 2) **Reduce inconsistencies in the resilience across the internal market in the sectors already covered by the NIS Directive**, by further aligning (1) the de-facto scope of the legal instrument, (2) the security and incident reporting requirements that public and private entities are required to put in place, (3) the provisions governing national supervision and enforcement and (4) the capabilities of competent authorities in the Member States.
- 3) **Improve the level of joint situational awareness and the collective capability to prepare and respond**, by taking measures aimed at increasing the level of trust between competent authorities, by sharing more information and by putting in place rules and procedures in the event of a large-scale incident or crisis.

These objectives are interrelated:

- **Synergies:** Reducing internal market fragmentation would contribute to increasing the level of cyber resilience in Member States as public and private entities subject to less stringent requirements would have to adhere to stricter rules. In addition, measures aimed at increasing the level of joint situational awareness would also have a positive impact on the level of resilience of public and private entities as such entities would benefit from the cooperation between competent authorities.
- **Trade-offs:** enhancing security could entail additional costs and constraints to the digital single market. For example, the implementation of increased security measures could bring additional costs to businesses, which could have a negative impact in their operations, in particular for SMEs.

### 5.2. Specific objectives

The specific objectives are defined for each area for which problems and problem drivers were described.

*To address the problem of low level of cyber resilience of businesses operating in the European Union*

1. Ensure that entities in all sectors that are dependent on network and information systems and that provide key services to the economy and society as a whole are required to take cybersecurity measures and report incidents with a view to increasing the overall level of cyber resilience throughout the internal market

*To address the problem of inconsistent resilience across Member States and sectors*

2. Ensure that all entities that are active in sectors covered by the NIS legal framework and that are similar in size and have a comparable role are subject to the same



regulatory regime (are either inside or outside the scope) no matter under which jurisdiction they fall within the EU

3. Ensure that all entities that are active in sectors covered by the NIS legal framework are required to follow aligned obligations based on the concept of risk management when it comes to security measures and must report incidents based on a uniform set of criteria
4. Ensure that competent authorities enforce the rules laid down by the legal instrument more effectively through aligned supervisory and enforcement measures
5. Ensure a comparable level of resources across Member States allocated to competent authorities that would allow them to fulfil the core tasks laid out by the NIS framework

*To address the problem of joint situational awareness and lack of joint crisis response*

6. Ensure that essential information is exchanged between Member States by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents and by developing a Union joint operational crisis response capacity

A review should evaluate in how far these objectives have been achieved within 54 months after coming into force.

## **6. WHAT ARE THE AVAILABLE POLICY OPTIONS?**

### **6.1. Description of the policy options**

This section presents the policy options, including the baseline scenario, that have been considered for addressing the problems identified in *Section 2* and meeting the objectives set out in *Section 5*.

The policy options analysed are designed based on the degree and nature of a potential intervention and in a ‘package’ format that groups envisaged actions and measures in the main areas that are already included or considered for being included in the NIS framework: (1) the sectoral scope and coverage of entities; (2) security requirements and reporting obligations (3) supervision and enforcement; (4) cooperation and information sharing (including the aspects relating to crisis management).

The actions and measures envisaged in the areas of intervention, which correspond to the specific objectives, are interrelated and linked to the type and degree of intervention. The policy options are, therefore, developed as a unified set of actions and measures in the above-mentioned areas which function as a whole: the policy choice made in one area being dependent on the choices made in the others. Furthermore, the description of each policy option includes a reference to the synergies with other related instruments, including sector-specific legislation or policies.

The list of actions and measures in the areas of intervention analysed within the policy options was developed with the purpose of putting forward viable alternatives. The description of each policy option therefore refers to potential alternatives for the areas of intervention that were not considered viable and explains the reasons why.

The intervention logic and the links between problem drivers, specific objectives and policy options is illustrated by *Table 1 below*. *A more detailed table with an overview of the policy options and their correspondence with the specific objectives is also included in Annex 8.*

		Policy options			
Problem drivers	Specific policy objectives	PO0 (status quo)	PO1 (non-legislative)	PO2 (limited changes)	PO3 (subst. changes)
<b>DR1:</b> Lack of cybersecurity measures taken by key companies	<b>SPO1:</b> Entities in NIS-dependent sectors to take measures and report incidents	Keep scope, requirements and obligations. Continue existing CG and CSIRTs network work	Keep scope, requirements and obligations + guidance	Extend scope with OES and DSP categories	Extend scope and introduce categories essential and important with different requirements
<b>DR2.1:</b> Discrepancies in OES identification and DSP coverage	<b>SPO2:</b> Similar entities in covered sectors subject to the same regulatory regime				
<b>DR2.2:</b> Inconsistent security measures and reporting requirements	<b>SPO3:</b> Entities to follow aligned security and reporting obligations	Guidelines on security and incident reporting requirements	Guidelines on security and incident reporting requirements	Harmonize security and reporting requirements	Introduce uniform security and reporting requirements —Explicit incident reporting rules
<b>DR2.3:</b> Ineffective supervision and enforcement	<b>SPO4:</b> Competent authorities to enforce more effectively			Explicit incident reporting requirements	
		Guidelines on DSPs	Guidelines on DSPs	Subject DSPs to the same	Subjecting entities under the same

			supervision	rules as OES	category to the same regulatory regime — Important entities subject to a light-touch regime
<b>DR2.4:</b> Discrepancies in Member State capabilities	<b>SPO5:</b> Comparable level of resources allocated to authorities		Incentivise MS to adequately fund their competent authorities and other relevant structures	MS to take measures to ensure that the competent authorities have the necessary resources	Peer-review mechanism to assess the capabilities of MS
<b>DR3.1:</b> Voluntary nature of cooperation	<b>SPO6:</b> Essential information to be exchanged between MS by introducing clear obligations and by developing a joint operational crisis response capacity	Continue existing work of the Cooperation Group and the CSIRTs network	— Further develop SOPs by the Cooperation Group and the CSIRTs network. — Launch CyCLONE, without a set legal framework.	Mandate or incentivize information sharing for competent authorities and companies (ISACs, PPPs)	— Mandatory mutual assistance and cooperation — Voluntary info sharing through ISACs and PPPs — MS to develop CVD policies — ENISA as state of cybersecurity observatory — Regular reports on the state of cybersecurity
<b>DR3.1:</b> Limited information feeding into the existing groups					
<b>DR3.1:</b> No crisis management structures					Crisis management framework, for both national and EU levels, including institutionalising CyCLONE

**Table 1:** *intervention logic*

### ***Option 0: Baseline scenario – maintaining the status quo***

In this scenario, the NIS Directive would remain unchanged and no other measures of non-legislative nature would be taken to target the problems identified by the evaluation of the NIS Directive. A more sector-specific shift could be expected in this scenario, advancing sectoral legislation that would also include cybersecurity aspects. The Cooperation Group and the CSIRTs network would continue the activities in line with their mandates, leading to further voluntary information sharing, exchange of practices and development of reference documents and guidance. The Cooperation Group would continue expanding to sector-specific work streams.<sup>100</sup> However, in the medium and long term, the drivers of cybersecurity policies at EU level would mainly stem from other related legal acts and policy measures, be them sector-specific or cross-sectoral. This would maintain the fragmented approach on cybersecurity across the EU, with more ad hoc solutions and less coherent responsibility sharing.

In particular, in the areas covered by the specific objectives (*section 5.2.*) the following main developments would be expected:

#### ***1. Sectoral scope and coverage of entities***

The **sectors and services** that fall under the **scope** of the NIS Directive would remain unchanged. In this scenario, it is expected for a subset of Member States to identify OESs in certain sectors, while the imbalance in key operators' preparedness would deepen, with potential negative consequences for the internal market. Sectors and services which have developed interdependencies with other essential sectors or have proven essential in times of COVID-19 crisis, would remain outside the NIS scope. 67% of the competent authorities responding to the NIS review study survey considered that the NIS Directive does not effectively cover all relevant (sub)sectors essential for the economy and society as a whole.

The **OES identification process and the DSP coverage** would remain unchanged. Some further guidance could be expected as part of the Cooperation Group's work, as well as via the EU Agency for Cybersecurity (ENISA). No change in the identification process would perpetuate or potentially amplify existing shortcomings.<sup>101</sup>

The sectoral work streams of the Cooperation Group are expected to further expand and more sector-specific guidance issued. Some further sector-specific legislation (e.g. in relation to energy or transport) may also be expected. Relying on only sector-specific initiatives is likely to have very little impact on the overall level of cross-sector and cross-border cyber resilience in the EU. Cyberattacks and vulnerabilities are often not sector- or country-specific. *More information on cross-sector and cross-border propagation of incidents is included in Annex 9.*

#### ***2. Security requirements and reporting obligations***

The current system for setting the security requirements and the thresholds for incident notifications would remain unchanged. Further guidance on these aspects is expected through the work of the Cooperation Group and ENISA. However, this would not be

---

<sup>100</sup> Currently there are sector-specific work streams on energy, elections and, more recently, health. More such work streams (including on subsectors) are potentially considered in the medium term.

<sup>101</sup> Such as major hospitals in a Member State not being identified as essential service operators, while in another Member State almost every health care facility in the country was identified as such. Or similarly major railway operator being subject to NIS requirements, while others not.

likely to effectively address the problems identified in practice and highlighted in *section 2.1*.

76% of the OES responding to the NIS review study survey faced challenges in implementing the NIS security requirements, while 71% consider that the misalignment of security requirements is among the main shortcomings of the current NIS Directive. This matches the views of the competent authorities.<sup>102</sup>

Currently there is a very low number of reported incidents.<sup>103</sup> Each year a number of Member States report zero incidents, while the majority report very low numbers. Very few Member States (on average 5) report incidents concerning DSPs. The last two years did not show any notable improvement and it is highly likely that, without a change in the common denominator and clarity of reporting obligations, no conclusive picture of incidents, underlying causes, typology and effects may be drawn at EU level.

### **3. Supervision and enforcement**

The approaches towards **supervision and enforcement** at Member State level would remain unchanged and uneven. The **light-touch approach on the DSP supervision** would be maintained.

The Cooperation Group could issue guidelines on such approaches, but given the differences encountered so far and how little enforcement systems have been used, it appears as highly unlikely for such guidance to increase alignment across the EU on these matters. 70% of respondents to the NIS review study surveys targeting competent authorities considered that their supervisory powers are effective only to some or to a moderate extent.<sup>104</sup> By perpetuating the current approach towards the supervision and enforcement system, it is unlikely the addressees of the NIS requirements would be dissuaded from non-compliant behaviour.

The differences in the **Member States' capabilities** are likely to be largely maintained, depending also on the evolution of national economies, as well as the political will at national level at any given moment and the priority given to cybersecurity on the political agenda. The NIS review country visits revealed insufficient resourcing of competent authorities and CSIRTs in a number of Member States, with adverse effects on the build-up of cybersecurity capabilities and trust among authorities across borders.<sup>105</sup> The cybersecurity competence centre and its related network, as well as the funds made available through Digital Europe and Horizon Europe programmes, would have a certain impact in this regard, but they cannot compensate for the level of cybersecurity policy prioritisation and political will at national levels.

### **4. Cooperation and information sharing**

In terms of **cooperation and information sharing** of public authorities and private entities, this would remain largely voluntary. The Cooperation Group and the CSIRTs

---

<sup>102</sup> 72% considered that the misalignment of the security requirements is a pressing issue.

<sup>103</sup> 78% of the competent authorities responding to the NIS review study survey considered that there is a need for streamlining incident notification obligations. 71% of OES and 55% of DSP responding to the survey were of the same opinion.

<sup>104</sup> In some Member States where the supervisory powers and corresponding means were prioritized and the resources and capabilities of the competent authorities matched the potential of these powers, benefits could have been seen in a pro-active approach of competent authorities and measures such as offering of vulnerability scans to companies leading to a good cooperation between businesses and competent authorities, trust and additional incentives to comply with security requirements.

<sup>105</sup> 63% of the respondents to the NIS review targeted survey for competent authorities considered that there is insufficient staffing and 50% that there are insufficient resources to ensure to a great or at least a moderate extent an effective fulfilment of their tasks.

network would also continue to function within the existing mandate.

Information sharing, for both national authorities and private entities, appears to take place scarcely.<sup>106</sup> At operational level, a survey conducted by ENISA in July 2020 among the CSIRTs network revealed that, while the network is overall satisfied with its activities, it considers that more needs to be done to improve operational information exchange and operational support in addressing cross-border incidents. Currently, there are seven sector-specific ISACs identified at EU level<sup>107</sup> and the tendency is to encourage the setting up of more such partnerships, both at EU level and at national level. Without a clearer framework for information exchange, the impact of these developments is likely to be limited and dispersed in time.

As regards **crisis management**, currently there is no established European framework for cybersecurity crisis management. Building on the Blueprint Recommendation issued based on the NIS framework, CyCLONe is being developed at operational level. Member States largely support this initiative and have already designated their contact points in CyCLONe, even if the structure is only voluntary. While this project is materialising, it would still benefit from a legal framework as a basis to ensure coherence, structure and certainty. In the NIS review consultations, a third of the Member States raised the need for formalizing CyCLONe within the NIS framework, clarifying the links between CyCLONe (operational level) and the CSIRTs network (technical level), and considering establishing an EU crisis management framework within the NIS context.

At political level, crisis management is carried out through horizontal instruments, such as the Council Integrated Political Crisis Response (IPCR) arrangements (for Member States), the Commission ARGUS<sup>108</sup> high-level cross-sectoral crisis coordination process (for the Commission) and the EEAS Crisis Response Mechanism. The EU civil protection mechanism<sup>109</sup>, which aims to improve prevention, preparedness and response to disasters, does not have a cybersecurity focus.

##### 5. Synergies with other related instruments

The NIS Directive provides for a *lex specialis principle*<sup>110</sup>, establishing that where a sector-specific Union legal act provides for equivalent cybersecurity requirements or incident notification obligations, the latter shall apply. This principle is, for example, currently applicable in the case of the security requirements and notification obligations for payment service providers as stipulated in the Directive on **payment services** in the internal market ('PSD2')<sup>111</sup>.

The proposal for a **Digital Operational Resilience Act (DORA)** for the financial sector, if adopted, will also represent such *lex specialis* for all financial services as it provides

---

<sup>106</sup> 83% of the respondents to the NIS review targeted survey for competent authorities considered that there is insufficient clarity and framework for addressing the challenges of cross-border dependencies, including outside the EU. 55% of the respondents to the OES-related survey considered the same. 65% of the respondents to the survey concerning the competent authorities consider that there is limited information sharing between Member States, potentially hampering the effective handling and prevention of incidents. 57% of the respondents to the surveys targeting OESs were of the same opinion.

<sup>107</sup> four of which in the transport sector.

<sup>108</sup> general rapid alert system linking all the European Commission's specialised systems for emergencies.

<sup>109</sup> [https://ec.europa.eu/echo/what/civil-protection/mechanism\\_en](https://ec.europa.eu/echo/what/civil-protection/mechanism_en).

<sup>110</sup> Article 7(1).

<sup>111</sup> 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 (Text with EEA relevance).

detailed provisions on security requirements and reporting obligations. The DORA framework envisages a one-stop-shop, proposing a system of reporting major ICT-related incidents to competent authorities in the financial sector which in their turn would notify the NIS single points of contact

Nevertheless, the *lex specialis* provisions of the NIS Directive have also triggered certain interpretation challenges in practice. Thus, certain Member States included under the NIS scope sectors where specific regulations provided also for cybersecurity requirements.

In addition, security-related obligations are provided in some other EU instruments, such as those concerning the public **electronic communication providers** in the European Electronic Communications Code<sup>112</sup> or the Regulation on electronic identification and **trust services** for electronic transactions in the internal market (eIDAS). These services are now excluded from the scope of the NIS Directive.

Another related EU legal instrument is the Directive on the **European Critical Infrastructure (ECI)**.<sup>113</sup> The ECI Directive is limited only to infrastructures the destruction or disruption of which would have a significant cross-border impact. The ECI Directive is therefore limited to physical protective arrangements. While both critical (physical) infrastructures and network and information systems are by their nature crucial to the provision of essential services, the ECI Directive is focused on the protection of specific assets that provide certain essential services; instead, the NIS Directive takes a broader approach that aims at ensuring a high and common level of security for the essential services as such (some of which are provided by infrastructures designated as ECIs). A review of the ECI Directive is envisaged. The envisaged ECI revision aims to replace the current ECI Directive with an **overarching cross-sectoral framework** to enhance the resilience of operators of essential services in the sectors covered by the NIS Directive, as well as telecommunications and space. The envisaged initiative is complementing the NIS Directive, avoiding overlaps. It would entail a different material approach and different types of measures and means which complement each other. The ECI framework would establish minimum requirements to address non-cyber threats for operators defined as critical as it focuses on enhancing the security of physical assets against threats such as terrorism and other intentional and unintentional man-made threats, as well as natural hazards.<sup>114</sup>

### ***Option 1: Non-legislative measures to align the implementation of the NIS Directive***

In this scenario, there would be no changes at legislative level. Instead, the Commission would issue recommendations and guidelines, upon consultation of the Cooperation Group, ENISA and, as applicable, the CSIRTs network. In particular, aside the developments described in the baseline scenario, which are also expected in this option, the following additional measures and/or developments are expected:

#### ***1. Sectoral scope and coverage of entities***

In this policy option, the **sectoral scope** of the NIS Directive, the **OES identification process** and the **DSP coverage** would remain unchanged, same as in the baseline scenario. At the same time, the sectoral work streams of the Cooperation Group

---

<sup>112</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

<sup>113</sup> Council 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.

<sup>114</sup> A possible overlap, however, arises from the fact that under the ECI Directive the designated ECIs should include measures on security of information systems as part of their Operator Security Plan (Annex 2 of the ECI Directive).

corresponding to the current scope are expected to further expand and more sector-specific guidance could be issued in this context, including by the Commission, in cooperation with various work streams of the Cooperation Group and ENISA. Further sector-specific legislation would also be expected, as in the baseline scenario.

In addition to the baseline scenario, more **guidance and recommendations** would be issued **by the Commission** on **sector-specific** aspects stemming from the differences in the **OES identification** process.

## *2. Security requirements and reporting obligations*

In this policy option, in addition to the expected developments in the baseline scenario, the **Commission would issue recommendations on security requirements or thresholds for incident reporting** and potentially **DSP-related** aspects, including jurisdiction issues.

## *3. Supervision and enforcement*

In this scenario, no changes would be expected as compared to the baseline scenario. The Commission is unlikely to issue recommendations to the Member States on these aspects since the current NIS Directive provisions are of very general nature in this respect and the discretion of the Member State is too wide. The Cooperation Group could potentially agree to issue certain guidelines on such approaches, but given the differences encountered in practice so far and the little use of the enforcement systems it appears as highly unlikely for such guidance to have a potential to raise the level of alignment across the EU on these matters. The **light-touch approach on the DSP supervision** would remain in force.

The differences in the **Member States' capabilities** are likely to be largely maintained, depending also on the evolution of the potency of national economies, as well as the political will at national level at any given moment and the priority given to cybersecurity on the political agenda

## *4. Cooperation and information sharing*

As in the baseline scenario, the cooperation among public authorities and private entities would remain largely of voluntary nature. The Cooperation Group and the CSIRTs network would also continue to function within the existing mandate.

In addition to the baseline scenario, the Commission may issue recommendations to encourage Member States to set up information-sharing frameworks or tools, such as Information Sharing and Analysis Centres – ISACs (with participation of public authorities) or other public private partnerships (PPPs). In this scenario, self-regulatory solutions within ISACs or PPPs could be incentivised and supported. However, self-regulatory solutions in a global digital environment have proven challenging. Giving more prominence to self-regulatory solutions as compared to regulatory intervention would raise additional fragmentation risks, with little evidence of effectiveness of supervision of security-related requirements in such a context. On a background where, as highlighted in *section 2.1.2*, inconsistent resilience across Member States and sectors was identified as a persistent problem, it appears that the alternative of a self-regulatory solution alone would not be viable.

## *5. Synergies with other related instruments*

The same developments as in the baseline scenario would be expected.



## ***Option 2: Limited changes to the current NIS Directive for further harmonization***

This scenario would entail targeted amendments to the NIS Directive, including an extension of the scope and several other amendments that would aim at guaranteeing certain immediate solutions to the problems identified, providing more clarity and further harmonization. The amended NIS Directive would however maintain the main building blocks, approach and rationale. In particular, the following measures and/or developments would be expected:

### ***1. Sectoral scope and coverage of entities***

**Additional sectors, subsectors and types of services** would be brought under the **scope**, within the two existing categories covered by the NIS Directive (OES and DSP).

The sectoral scope of the NIS framework should provide for a comprehensive coverage of the sectors and services of vital importance for key societal and economic activities within the internal market. The overall NIS review process, starting with the country visits, brought the attention to a considerable number of sectors and types of services which were not included under the scope of the NIS Directive, but which were nevertheless added or considered to be added to the NIS scope by the Member States or were frequently referred to in consultations with the relevant stakeholders. It became therefore evident in the early stages of the NIS review process that, should an extension of the NIS sectoral scope be considered, this would rather be a substantial one.

A **potential alternative** to a substantial extension of the NIS scope could have consisted of the addition of a number of subsectors to the already existing sectors listed in Annex I of the NIS Directive (such as: electricity generation, district heating or electricity market operators within the energy sector or social networks as part of digital service providers), jointly with the submission of trust services and public electronic communications networks and electronic communications services to the NIS scope, while repealing the cybersecurity-related requirements concerning these services provided by their respective EU legislation. Such an alternative would have however ignored the Member States' national policies to go beyond the scope of the current NIS Directive, the problems and challenges stemming from the increased interconnectedness and interdependencies among sectors, as well as the lessons learnt from the COVID-19 crises. For these reasons, a minimal expansion of the scope of the NIS framework was not considered a viable alternative for the policy options that would entail an amendment or a more systematic revision of the NIS framework (*i.e. options 2 and 3*).

### ***Selection of additional sectors and services to be covered by the NIS framework***

The additional sectors, subsectors and services considered for the NIS scope were determined based on the following **criteria** (*for detailed information on the methodology applied, see Annex 4*):

- existing Member States' policies covering sectors, subsectors and services beyond the scope of the NIS Directive;
- stakeholders' views reflected in the results of the OPC and the targeted surveys conducted by the NIS review study;
- sectoral digital intensity;
- level of importance for society of sectors, subsectors and services as revealed by a major crisis such as COVID-19;
- interdependency among sectors.

In deciding on which new sectors and types of services to be added to the NIS scope, an equal weight was given to each of the above-mentioned criteria. These criteria reflect elements ranging from national risk evaluations and stakeholders' views, up to practical implications of the COVID-19 crisis and more technical cyber-related aspects. Technical criteria such as digital intensity and interdependency among sectors could not have determined alone the importance of certain sectors or services for the societal and economic activities. For example, a sector such as healthcare, currently covered by the NIS Directive, would not score high on such technical criteria, while nevertheless being vital for society and at the same time vulnerable to cyber threats, as has also been proven in the context of the COVID-19 crisis. The Member States' national evaluations, which led to the consideration of additional sectors or services for the NIS scope, as well as the opinions of well-informed practitioners from both industry and public authorities who participated in the NIS review consultations, were therefore considered equally important as technical criteria such as interconnectivity or digital intensity. All these criteria also indicated cumulatively the level of vulnerability to cyber threats. Furthermore, the COVID-19 crisis has revealed, from a very practical perspective, the criticality of certain sectors and services for societies and economies, and was therefore added to the criteria assessed in view of a potential sectoral extension of the NIS scope.

The Open Public Consultation asked stakeholders representing the new sectors and services if they themselves should also be brought under the NIS scope. In most sectors, respondents tended to welcome the addition to the scope of the NIS Directive, including in public administration.<sup>115</sup>

The table below lists the additional sectors and types of services that scored high on a combination of the above-mentioned criteria and a qualitative analysis of criticality and exposure to cyber threats. Other (sub)sectors or services, such as insurance or education, were discarded for the sectoral scope extension at an early stage, due to their low scores on the above-mentioned criteria and the qualitative aspects. *See also Annex 4 for the analysis of the above-mentioned criteria.*

<b>No.</b>	<b>Sector/type of service</b>	<b>Criteria considered in view of inclusion in the NIS scope (in the order of scoring)</b>	<b>Qualitative aspects supporting the inclusion in the scope of the NIS framework</b>
1	Wastewater	<ul style="list-style-type: none"> <li>• Member States' national policies;</li> <li>• Results of consultations;</li> <li>• COVID-19 crisis.</li> </ul>	<p>Wastewater systems are essential for drinking water supply and distribution (a sector already covered by the current NIS Directive). Properly treated wastewater is vital for preventing disease and protecting the environment.</p> <p>Cyber-attacks on wastewater utilities or process control systems can cause significant</p>

<sup>115</sup> Both in food supply and manufacturing the results were more mixed, with only half of the respondents supporting the idea of being brought under the NIS scope. Social networks rejected the proposition. No responses were received from the heat, waste management and postal services sectors and from content delivery networks.

			harm, compromising the ability of water and wastewater utilities to provide clean and safe water to the population. If a waste treatment facility gets hacked, it may lead up to thousands of tons of raw sewerage flowing down a local river.
2	Data centre services	<ul style="list-style-type: none"> <li>• Digital intensity;</li> <li>• Interdependency with other sectors;</li> <li>• Member States' national policies;</li> <li>• Results of consultations;</li> <li>• COVID-19 crisis.</li> </ul>	Data centres services are key services in a data-centric economy. They enable data processing and storage (such as colocation or dedicated hosting) and hold proprietary and sensitive information such as intellectual property, customer data, and financial records, which are highly exposed to cyber threats. Data centres are also the physical infrastructure used for the provision of cloud-based services.
3	Content delivery network services	<ul style="list-style-type: none"> <li>• Digital intensity;</li> <li>• Interdependency with other sectors;</li> <li>• Member States' national policies;</li> <li>• Results of consultations;</li> <li>• COVID-19 crisis.</li> </ul>	Like data centres, content delivery networks are essential elements of digital infrastructure that play a key role in a data-centric economy. Today the majority of web traffic is served through Content Delivery Networks (CDNs). A CDN essentially replicates content to multiple places so that content becomes closer to the end users. Deployed on the edge of a network, a CDN is well-situated to act as a virtual high-security fence and prevent attacks on websites and web applications. The on-edge position also makes a CDN ideal for blocking DDoS floods.
4	Trust services	<ul style="list-style-type: none"> <li>• Digital intensity;</li> <li>• Interdependency with other sectors;</li> </ul>	Trust service providers are subject to security and reporting obligations under the eIDAS Regulation, which are

		<ul style="list-style-type: none"> <li>• Results of consultations.</li> </ul>	<p>similar to those laid down in the NIS Directive. However, digital certificates provided by those providers are frequently used as authentication factors in the provision of financial services, cloud computing services or other essential services that fall under the current NIS Directive. Therefore, any security incident affecting the trust services used as authentication means within the essential services might also affect the continuity of the essential service itself and thereby trigger a double reporting.</p> <p>The repeal of these obligations from the eIDAS Regulation and their inclusion under the revised NIS would streamline the legal obligations for those entities.</p>
5	Public electronic communications networks and electronic communications services (insofar as these are publicly available)	<ul style="list-style-type: none"> <li>• Digital intensity;</li> <li>• Interdependency with other sectors;</li> <li>• Member States' national policies;</li> <li>• Results of consultations;</li> <li>• COVID-19 crisis.</li> </ul>	<p>Electronic communications networks or services are subject to security and incident notification obligations laid down in Article 40 of the European Electronic Communication Code. At the same time, these providers are subject to almost identical type of obligations under the NIS Directive as far as they also provide services included in the NIS scope such as Internet Exchange Points, Domain Name Servers or cloud computing services.</p> <p>The repeal of these obligations from the European Electronic Communication Code and their inclusion under the revised NIS Directive would streamline the legal obligations for those entities.</p>
6	Postal and courier services	<ul style="list-style-type: none"> <li>• COVID-19 crisis</li> <li>• Member States' national</li> </ul>	Postal and courier services are key services for businesses,

		<p>policies;</p> <ul style="list-style-type: none"> <li>• Results of consultations;</li> <li>• Digital intensity;</li> <li>• Interdependency with other sectors</li> </ul>	<p>citizens and public services, including democratic processes such as elections. The disruption of such services, denial of service or intrusions leading to data breaches as a result of cyber attacks may cause considerable damage to societies and economies. The COVID-19 pandemic revealed once more the criticality of postal and courier services for societal and economic activities.</p>
7	Waste management	<ul style="list-style-type: none"> <li>• Results of consultations;</li> <li>• Member States' national policies;</li> <li>• COVID-19 crisis;</li> <li>• Interdependency with other sectors</li> </ul>	<p>Industrial companies that deal with hazardous materials (e.g. power plants, refineries, factories, water treatment facilities or pipelines) are using automated technology to maximize their efficiency.</p> <p>Damaging or even catastrophic environmental releases may be triggered remotely by cyber attacks.</p>
8	Manufacture, production and distribution of chemicals	<ul style="list-style-type: none"> <li>• Member States' national policies;</li> <li>• Results of consultations;</li> <li>• Digital intensity</li> </ul>	<p>Cyber attacks against the information and process control systems of chemical facilities can disrupt or shut down operations and lead to serious consequences, such as health and safety risks, including loss of life. Such attacks could potentially manipulate facilities' information and control systems to release or steal hazardous chemicals and inflict casualties.<sup>116</sup></p> <p>There has been a substantial increase in cyber threats on chemical industry information technology and production assets amid a wider spike in malicious activity as hackers</p>

<sup>116</sup> <https://www.msspalert.com/cybersecurity-markets/verticals/chemical-facilities-threatened-by-cyber-attacks/>

			seek to exploit new vulnerabilities created by shifts in work habits since the onset of the COVID-19 pandemic. <sup>117</sup>
9	Manufacturing (notably manufacture of: food products; beverages; basic pharmaceutical products and pharmaceutical preparations; research and development activities of medicinal products; medical devices and in vitro diagnostic medical devices (including medical devices considered as critical during a public health emergency); computer, electronic and optical products, electrical equipment, machinery and equipment n.e.c., motor vehicles, trailers and semi-trailers, other transport equipment)	<ul style="list-style-type: none"> <li>• Member States' national policies;</li> <li>• Results of consultations;</li> <li>• Digital intensity;</li> <li>• Interdependency with other sectors;</li> <li>• COVID-19 crisis</li> </ul>	<p>Manufacturing covers a very wide portion of economy and a very large number of areas and entities. Manufacturing companies are valuable targets for cyber attacks, mainly due to their sheer size, but also because they deliver products which other sectors, industries or citizens rely upon. Furthermore, they also have a lot of valuable data that can be targeted by cyber criminals.</p> <p>Cyber attacks on manufacturing companies can cause considerable disruptions and financial damage along the whole supply chain.</p> <p>As show by a study conducted by Deloitte and MAPI on cyber risks in advanced manufacturing<sup>118</sup>, the manufacturing companies' focus on innovation, the pace of technological change they face and an increasing reliance on connected products, makes them even more vulnerable to cyber risks.</p> <p>For the NIS framework, only the manufacturing of certain products was considered, linked to their criticality for societies and economies, and notably their level of interdependency with other sectors, as well as the importance revealed by the COVID-19 crisis and the</p>

<sup>117</sup> <https://www.icis.com/explore/resources/news/2020/06/17/10520231/insight-chemical-industry-faces-up-to-cybercrime-spike-amid-cost-cutting-pressures> .

<sup>118</sup> <https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html> .

			national policies of the Member States.
10	Food supply	<ul style="list-style-type: none"> <li>• Member States' national policies;</li> <li>• Results of consultations;</li> <li>• COVID-19 crisis;</li> <li>• Digital intensity.</li> </ul>	<p>Food supply is a fundamental pillar of societies. A shortage of food supplies would have catastrophic effects on societies. The COVID-19 crisis stressed even more the criticality of the food supply chain.</p> <p>In terms of technology, digital intensity and vulnerabilities to cyber threats, the food supply sector is not much different from other traditional industries, undergoing rapid industrial evolution. The industry is adopting new and not yet battle-tested technology with advanced sensors, robotics, drones and autonomous vehicles.<sup>119</sup></p> <p>Cyber threats can impact the food supply chain in many ways. Cyber attacks could: impede the movement of materials and ingredients from suppliers to manufacturers, target shipments of food, compromise IT and OT networks by ransomware, with the rapid spoilage of food in production being an incentive to pay the ransom. Shipments from manufacturers to customers could be delayed or re-routed to the wrong locations. Cybersecurity measures are therefore key to keeping systems and processes running, and food safe and the supply chain intact.<sup>120</sup></p>
11	Social networks	<ul style="list-style-type: none"> <li>• Results of consultations;</li> <li>• COVID-19 crisis;</li> </ul>	<p>Social networks have an increasing importance for societies, ranging from connecting people and</p>

<sup>119</sup> <https://www.securityweek.com/cybersecurity-threats-food-supply-chain> .

<sup>120</sup> <https://www.qad.com/blog/2020/09/why-cybersecurity-matters-in-the-food-and-beverage-supply-chain>

		<ul style="list-style-type: none"> <li>• Digital intensity.</li> </ul>	<p>businesses, up to social media and e-commerce, as well as influencing democratic processes and distribution of news and information.</p> <p>In 2020, 3.81 billion people worldwide were using social media. 49% of the total world population are using social networks.<sup>121</sup></p> <p>Digital consumers spend nearly 2.5 hours on social networks and social messaging every day.<sup>122</sup></p> <p>According to DESI<sup>123</sup>, social networks (51 %) were the most used form of social media platforms in 2019. Furthermore, 65% of internet users in the EU used social networks in 2019.<sup>124</sup></p> <p>Given the breadth of their coverage, reach out to users and implicitly big valuable data they entail, social networks are valuable targets for cyber attacks.</p> <p>Social media is primarily used by cybercriminals as an intelligence gathering tool, but it is also a threat vector itself<sup>125</sup>, notably when cybercriminals are spreading malware and misinformation.<sup>126</sup> For example, in May 2016, LinkedIn was hacked, and 117 million credentials were exposed. In 2017, Vevo fell</p>
--	--	--	--

<sup>121</sup> Kemp, Simon. "Digital 2020: April Global Statshot Report." We Are Social Inc. April 23, 2020. <https://wearesocial.com/blog/2020/04/digital-around-the-world-in-april-2020> and [https://www.cisa.gov/sites/default/files/publications/NCSAM\\_SocialMediaCybersecurity\\_2020.pdf](https://www.cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf)

<sup>122</sup> G., Deyan. "How Much Time Do People Spend on Social Media in 2020?" TechJury. June 18, 2020. <https://techjury.net/blog/time-spent-on-social-media/> .

<sup>123</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Social\\_media\\_-\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_-_statistics_on_the_use_by_enterprises)

<sup>124</sup> <https://ec.europa.eu/digital-single-market/en/use-internet> .

<sup>125</sup> <https://www.bridewellconsulting.com/cyber-trends-for-2020-social-media-attacks> .

<sup>126</sup> <https://versprite.com/blog/top-motives-hackers-attack-social-media-2020/> .



			victim to a phishing attack, and 3.12 terabytes of sensitive company data were affected. Twitter was hacked in July 2020, and influential accounts were used in a bitcoin theft operation. <sup>127</sup>
--	--	--	---

**Table 2:** selection of additional sectors and services for the NIS scope

In this policy option, operators of government-owned and privately-owned **ground-based infrastructure that support the provision of space-based services** would also be added to the NIS scope. Ground-based infrastructure performs essential functions, including control, monitoring, tracking and data collection activities. Space-based services are playing an increasingly important role for the economy and society as a whole and are important for the daily operations of many other essential and important entities. The sector exhibits a very high degree of digital intensity and its operators are highly interconnected with other parts of the economy, making them a likely target for cyber-attacks. Given the large economies of scale that prevail in the provision of space-based services, the sector also exhibits a particularly strong pan-European dimension.

Furthermore additional **subsectors** would also be added for the **energy sector**, and in particular: district heating, electricity generation, central oil stockholding entities, nominated electricity market operators and electricity market participants providing aggregation, demand response or energy storage services, operators of hydrogen production storage and transmission<sup>128</sup>, as well as EU reference laboratories and entities carrying out research and development activities of medicinal products for the **healthcare** sector.

**Public administration**, notably at the level of central government, major socio-economic regions and basic regions, would also be added to the NIS scope in this policy option, in its function of provider of services to citizens and businesses that are essential for the functioning of the internal market. The amended NIS Directive would not apply to public administration entities carrying out activities in the areas of the public security, law enforcement, defence and national security.

Mention should be made that, as the cybersecurity threat landscape is constantly evolving, it is not possible to **exclude sectors** from the NIS scope with complete certainty. However, those entities that would be excluded from the NIS scope would still benefit from the general measures provided by the NIS Directive and the wider cybersecurity policy framework. They can receive support and guidance stemming from the implementation of the national cybersecurity strategies, the services that national CSIRTs provide, guidelines issued by competent authorities, cybersecurity investment schemes at national level and the services provided by EU bodies (such as ENISA or the European Cybercrime Centre). In addition, market pressure exercised by consumers or supply-chain relationships will often force larger operators to put in place measures, even if not required by law to do so.

<sup>127</sup> Idem.

<sup>128</sup> The strategic vision for a climate-neutral EU envisages hydrogen as an important contributor to the EU energy mix by 2050 with a share of 13-14%. This position has been further fostered by the Communication “A hydrogen strategy for a climate-neutral Europe” [COM\(2020\) 301](#). Turning clean hydrogen into a viable solution to a decarbonised EU will necessarily demand a dedicated infrastructure of key importance for the new EU energy system and economy in general.

*List of all sectors and services to fall within the NIS scope in policy option 2*

In the light of the above, the table below illustrates the **sectors and types of services that would be covered by the NIS Directive in policy option 2**, including both those which currently fall within the scope of the NIS Directive and the new ones that would be added under this policy option under each category (i.e. OES and DSP).

<i>Sectors and subsectors for the OES currently under the scope of the NIS Directive which will also remain under option 2</i>		<i>New sectors and subsectors for OES considered to be <u>added</u> to the NIS scope</i>		<i>Types of DSPs currently in the scope of the NIS Directive</i>	<i>New types of DSPs considered to be <u>added</u> to the NIS scope</i>
Energy	Electricity (supply, distribution, transmission)	Energy	Electricity generation	Online marketplaces	Social networks
	Oil		(Nominated) electricity market operators		
	Gas		Central oil stocking entities <sup>129</sup>		
			Electricity market participants providing aggregation, demand response or energy storage services <sup>130</sup>		
	Operators of hydrogen production storage and transmission <sup>131</sup>				
Transport	Air	Heat production and supply		Online search engines	Trust service
	Rail				

<sup>129</sup> As defined in point (f) of Article 2 Directive 2009/119/EC.

<sup>130</sup> The inclusion in the NIS scope of electricity market participants as defined by Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services, as defined by Directive (EU) 2019/944 was considered notably due to their importance for the energy sector and the Green Deal.

<sup>131</sup> Communication “A hydrogen strategy for a climate-neutral Europe”.

	Water				providers
	Road				
Banking		Chemicals (manufacture, production and distribution)		Cloud computing services	
Financial infrastructures	market	Food supply <sup>132</sup>			
Health (healthcare providers)	Health	EU reference laboratories <sup>133</sup>			
		Entities conducting research and development activities of medicinal products <sup>134</sup>			
		Wastewater systems			
Drinking water distribution and supply		Waste management			
Digital infrastructure	Internet Exchange Points (IXPs)	Digital infrastructure	Data centres		
	Domain Name Server (DNS) service providers <sup>135</sup>		Content Delivery Network providers		
	Top Level Domain (TLD) name registers				

<sup>132</sup> As regards the food sector, food supply is complemented by the sub-subsector of manufacture of food products, as explained below in relation to the whole manufacturing sector (footnote 137). Therefore, the overall food sector to be covered would concern food production, processing and distribution.

<sup>133</sup> As defined by Article 15 of the Proposal for a Regulation of the European Parliament and of the Council on serious cross-border threats to health, repealing Decision 1082/2013/EU.

<sup>134</sup> Research and development activities of medicinal products (as defined in Article 1 point 2 of Directive 2001/83/EC of the European Parliament and of the Council on the Community Code relating to medicinal products for human use);

<sup>135</sup> In this option, the DNS definition would be further clarified and would also specify, among others, that root server providers are included in this category.

	Providers of electronic communications networks or of publicly available electronic communications services <sup>136</sup>		
	Postal and courier services		
	Manufacturing (certain subsectors) <sup>137</sup>		
	Public administration <sup>138</sup>		
	Operators of government-owned and privately-owned ground-based infrastructure that support the provision of space-based services <sup>139</sup>		

**Table 3:** sectors, subsectors and services that would fall under the NIS scope under policy option 2

As regards the **OES identification process** and **DSP coverage**:

- ✓ The **OES identification process** would remain in place. However, the NIS Directive

<sup>136</sup> These services would be added to the scope of the NIS Directive and taken out of the scope of the cybersecurity-related obligations provided by the European Electronic Communication Code. Consequently, the security provisions of the Code (i.e. Articles 40 and 41) would be repealed.

<sup>137</sup> The subsectors of manufacturing selected were chosen based on the same criteria as those applied to the overall selection of new (sub)sectors and services: i.e. existing Member States' policies covering subsectors beyond the scope of the NIS Directive; stakeholders' views reflected in the results of the OPC and the targeted surveys conducted by the NIS review study; sectorial digital intensity; level of importance for society of sectors, subsectors and services as revealed by a major crisis such as COVID-19; interdependency among sectors. Based on these criteria, the following manufacturing sub-sectors would be covered: food products; beverages; basic pharmaceutical products and pharmaceutical preparations; medical devices and in vitro diagnostic medical devices (as defined in point 1 of Article 2 of Regulation 2017/745 of the European Parliament and of the Council on medical devices, and entities manufacturing in vitro diagnostic medical devices as defined in point 2 of Article 2 of Regulation 2017/746 of the European Parliament and of the Council), as well as medical devices considered as critical during a public health emergency (according to Article 20 of the Commission Proposal for a [Regulation on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (COM92020)725 final); computer, electronic and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers and semi-trailers; other transport equipment.

<sup>138</sup> The NIS framework would cover under 'public administration' central governments (i.e. all administrative departments of the state and other central agencies whose responsibilities cover the whole economic territory of a country), as well as the major socio-economic regions (104 in total according to the NUTS 2021 classification) and the basic regions for the application of regional policies (283 in total according to the NUTS 2021 classification). It can also be considered to include election authorities, technology and processes, which are functional for limited periods of time.

<sup>139</sup> with the exception of specific ground-based infrastructure that directly supports space-based components of the EU's space programme, including Galileo, EGNOS, Copernicus, GOVSATCOM and Space Surveillance and Tracking.

would be amended to harmonise identification thresholds cross-sectors.<sup>140</sup>

- ✓ The **DSP coverage rules** would remain the same, i.e. there would be no identification process for the DSPs.<sup>141</sup> Further clarifications would be introduced in relation to the **jurisdiction rules**<sup>142</sup>.
- ✓ **Some DSPs** (e.g. **providing services to OES**, *such as cloud service providers*) would be **subject to the same regulatory regime as OES**: i.e. same security requirements and reporting obligations and subject to a fully-fledged supervisory and enforcement system. The so-called ‘light-touch’ approach in relation to these DSPs would therefore be removed.

Even with a more inclusive NIS scope under this option, the shortcomings generated by the identification process for the entities that need to be covered from a cybersecurity perspective would remain. The overall identification system would remain complex, engage considerable resources on the part of national competent authorities and would not be expected to lead to a notable increase in the number of identified OESs.

As regards the number and extent of coverage of the **entities**<sup>143</sup> **active in the sectors, subsectors and services** currently covered by the NIS Directive, in this option it is expected for competent authorities to supervise a similar number of operators as the ones that are currently identified as OES: i.e.<sup>144</sup> 872 OESs in the **energy** sector, 620 OESs in **transport** (air, water, rail and road), 822 OESs in the **drinking water and supply distribution** sector, 12,469 OESs in the **health** sector, 411 OESs in the **banking** sector, 172 OESs in **financial market infrastructures** and 173 OESs in **digital infrastructure**.

As regards the **entities active in the new sectors, subsectors and services** considered in this option:

- ✓ The **providers of electronic communications networks or of publicly available electronic communications services**<sup>145</sup> and **trust service providers** would be added to the amended NIS scope. There are 37,204 telecom providers and 7,775 programming and broadcaster providers and 190 active qualified trust service

---

<sup>140</sup> See also policy option 3 for an assessment of the alternative measure of harmonisation of identification thresholds.

<sup>141</sup> Instead, in this scenario, the definition of certain DSPs (such as IXP providers) would be further clarified and adjusted.

<sup>142</sup> notably on the rules concerning the ‘main establishment’, ‘one legal entity’, as well as the rules applicable for DSPs with the main establishment outside the EU.

<sup>143</sup> The data on the entities active in the (sub)sectors and services covered by or considered for the NIS scope are presented in detail in Annex 3. Mention should be made that the data analysed was based mainly on Eurostat and DESI data. Similar data was not available across the EU for all (sub)sectors or services analysed. Furthermore, the data was often available in aggregate forms which do not always entirely match the types of entities defined under the NIS scope, therefore in most cases the overall figures represent an overestimate. Whenever systematic data on number of companies and turnover were not available, proxies were used to the extent possible, including data or information on market structure or market shares. The data and estimates used by this impact assessment provide therefore a meaningful, yet not comprehensive overview of the above-mentioned metrics. For the sectors currently covered by the NIS scope, a comparison was made with the number of OES notified by the Member States by October 2020. For all the data sourced from Eurostat (notably number of companies, including medium and large, turnover and average turnover per company), the data used (as the most recent available) is from 2018. If specific sources are not mentioned, it should be assumed that the source of the data is Eurostat.

<sup>144</sup> Data based on notifications from the Member States pursuant to Article 5(7) of the NIS Directive.

<sup>145</sup> Broadcasting services and emergency communication services are also considered under this sector.

providers operating in 28 of the 31 EU and EEA/EFTA countries.<sup>146</sup>

- ✓ For new sectors considered, the number of entities<sup>147</sup> concerned would be as follows: i.e. for **manufacture of chemicals and chemical products**: 3,845 companies; for **waste management** (waste collection, treatment and disposal activities): 44,189 companies; for **wastewater** (sewerage): 10,955 companies; for **postal and courier services**, 89,480 companies; for **food supply**<sup>148</sup>: 595,233 companies; for **manufacturing, for 8 selected subsectors** (other than chemicals)<sup>149</sup>: 402,851 companies. Since the OES identification system would still apply, it would be expected for the number of OESs eventually identified to be much lower than the total number of entities mentioned above. However, the competent authorities would still need to process for identification purposes a large number of new entities.
- ✓ As regards **energy** (electricity generation), there are about 3,944 companies (representing at least 95% of the national net electricity generation in the EU) and 82 main electricity generating companies. For heat production and supply, no granular data was available on the number of companies. Heating and cooling accounts for approx. 46% of Europe's final energy demand.<sup>150</sup> In EU households, heating and hot water alone account for 79% of total final energy use.<sup>151</sup> As regards central oil stocktaking, there are 23 entities in Europe. There are 13 nominated electricity market operators in Europe.
- ✓ **Data centres** provide different types of services enabling data processing and storage (such as colocation or dedicated hosting). Some large companies also operate their own data centres. Data centres are also the physical infrastructure used for the provision of cloud-based services. This is a highly concentrated market in Europe, with Frankfurt, London, Amsterdam and Paris (so-called FLAP) dominating. Market players, such as Equinix or Interxion, include global companies, but also medium and large firms focusing on the European market. The **content delivery networks** market is also dominated by major providers, non-headquartered in the EU; in 2016, 95 % of global CDN traffic for web-based apps was delivered by 10 companies. From the perspective of the supervision of entities, in both option 2 and 3, the addition of this type of entities is not expected to generate burden, other than the need to further clarify the jurisdiction rules for non-EU based players, which would be addressed in both options. The same is valid for the **social networks**, with very few European-based providers. Facebook has a market share in social media of over 70% and at times over 80% in 2019-2020, followed by Pinterest, Twitter and Instagram with less than 12% and other players such as Youtube, Tumblr, Vkontakte with less than 1%<sup>152</sup>

## 2. Security requirements and reporting obligations

The **security requirements and incident reporting obligations** for OES would be further harmonised via the amendments to the NIS Directive and delegated acts. More

---

<sup>146</sup> The European List of Trusted Lists (LOTL), sourced from the Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020.

<sup>147</sup> According to Eurostat data corresponding to 2018, as presented in Annex 3.

<sup>148</sup> The data represent an overestimate, since they also cover wholesale and retail of tobacco, which would not be included in the NIS scope in policy options 2 and 3.

<sup>149</sup> food products; beverages; basic pharmaceutical products and pharmaceutical preparations; computer, electronic and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers and semi-trailers; other transport equipment.

<sup>150</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity\\_and\\_heat\\_statistics&oldid=493775#Derived\\_heat\\_production](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_and_heat_statistics&oldid=493775#Derived_heat_production)

<sup>151</sup> [https://ec.europa.eu/energy/topics/energy-efficiency/heating-and-cooling\\_en?redir=1](https://ec.europa.eu/energy/topics/energy-efficiency/heating-and-cooling_en?redir=1)

<sup>152</sup> <https://gs.statcounter.com/social-media-stats/all/europe>

clarity would therefore be provided for businesses, competent authorities and CSIRTs, creating the premises for an increase in the reporting rates and a better situational awareness. More specifically:

- ✓ On **security requirements**, a risk management approach would be applied. The amended NIS Directive would provide for a minimum list of basic elements which shall be part of the measures that OESs and DSPs must take to prevent and minimise the impact of cybersecurity incidents on users and other networks and services. Such elements would refer to, among others: risk analysis and information system security policies, incident handling, business continuity and crisis management, cybersecurity testing, cryptography and encryption, etc. The Commission would be empowered to issue delegated acts for further specifying and supplementing these elements.<sup>153</sup> The **alternative** of having more prescriptive security requirements in this policy option was discarded at an early stage, since it would have not allowed sufficient flexibility to take account of the sector-specific aspects or the fast-pace technological advancements.
- ✓ On **reporting obligations**: more precise provisions would be introduced on modalities, content and timelines of the reporting process. In particular, the amendments to the NIS Directive would clarify the definition of significant incidents that must be reported to competent authorities, as well as how these should be reported (i.e. timing – within what deadlines – and content of notification – what information related to the incident). Furthermore, in this scenario, cyber threats that could have likely resulted in a significant cybersecurity incident would also be reported. The notification of near misses<sup>154</sup> would be on a voluntary basis. The Commission would be empowered to issue delegated acts for specifying and supplementing these elements. No other **alternatives** that would have entailed a centralised reporting system at EU level or a mandatory reporting of all events, including near missed and vulnerabilities, were considered viable in this policy option, since they would have put a disproportionate burden on both businesses and competent authorities and would not have been expected to yield more effective results in terms of compliance with the notification obligations or cyber resilience.

### ***3. Supervision and enforcement***

As regards **supervision and enforcement**:

- ✓ On **supervision**, amendments to the NIS Directive would further clarify the principles applicable to the supervisory actions and the typical means through which competent authorities would exercise their supervisory powers, without establishing minimum requirements in this regard. The amendments to the NIS Directive would therefore provide for principle-based requirements for supervisory activities, namely the obligation of the Member States to ensure that competent authorities have the necessary powers and means to assess compliance with the NIS obligations and that they can require the entities under the extended NIS scope to provide any information necessary to assess the cybersecurity measures, access to data, documents and/or information necessary for the performance of the supervision or evidence of implementation of security policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.
- ✓ On **enforcement**, the amended NIS Directive would define the main principles and elements based on which Member States would establish sanctions (e.g. defining the

---

<sup>153</sup> taking account of new cyber threats, technological developments or sectorial specificities.

<sup>154</sup> events which can potentially cause harm but were successfully prevented from being unfolded fully.

circumstances to be considered when deciding on types of sanction to apply). In particular, the amended NIS Directive would define the circumstances to be considered by the competent authorities when establishing sanctions, such as the seriousness and duration of the infringement, the intentional or negligent character of the infringement, the actual damage caused, the preventive measures put in place to mitigate the damage, the level of cooperation with the competent authorities, etc.

A more prescriptive supervision and/or enforcement system would not have been a viable **alternative** in this policy option, notably since it would have not realistically matched the discretion that would still be left to the Member States in determining the entities that fall within the NIS scope through a complex identification system.

In relation to the **resources** available for the functioning of the competent authorities, the NIS Directive would more explicitly require Member States to take the necessary measures to ensure that the competent authorities have the technical, financial and human resources necessary to fulfil their mandate.

#### **4. Cooperation and information sharing**

In this option, the amendments to the NIS Directive would:

- ✓ encourage Member States to set up information-sharing frameworks or tools, such as Information Sharing and Analysis Centres – ISACs (with participation of public authorities) or other public private partnerships (PPPs).
- ✓ reinforce the Cooperation Group mandate to provide additional tools<sup>155</sup> for the support of EU cybersecurity policies and help strengthening capabilities at Member State level and across the Union. More specifically, in addition to the activities provided in its current mandate, the Cooperation Group would: (i) facilitate the exchange of national officials through a capacity building programme, (ii) discuss capabilities and preparedness of Member States, (iii) help<sup>156</sup> coordinate the Union response to current and emerging policy challenges. An EU cybersecurity stakeholders' forum would be set up to engage regularly with various stakeholders, including businesses and associations, and advise on emerging cybersecurity aspects.
- ✓ strengthen the **CSIRTs network's mandate** to allow, in addition to its current mandate, more information sharing, joint actions<sup>157</sup> and assistance among Member States to reinforce capabilities. This would include exchange of information on vulnerabilities that affect multiple organisations established in more than one Member State.
- ✓ introduce more specific provisions on the **collaboration between the Cooperation Group and the CSIRTs network**, including on the strategic guidance that the Cooperation Group would provide to the network and information flows.

No other **alternative** that would have entailed mandatory information sharing systems for both businesses and among competent authorities cross-border were considered viable in this policy option. This is mainly due to the approach taken in this option towards the identification process of OESs, where a large discretion is left to the Member States, and the security and reporting obligations (i.e. principle-based rather than overly prescriptive), which would not have supported a mandated information sharing. Furthermore, in a policy area such as cybersecurity, where trust is a key aspect, it is unlikely that mandatory information sharing could force such trust and deliver results.

---

<sup>155</sup> including secure information sharing tools.

<sup>156</sup> through guidelines, opinions.

<sup>157</sup> such as: joint investigations, publication of reports, common position on standards' development.



As regards **crisis management**, the CyCLONe network would continue functioning strictly on a voluntary basis, as in the baseline scenario, without an established legal basis and without established obligations for the Member States in relation to crises management frameworks and cooperation at national and EU levels.

### 5. *Synergies with other related instruments*

In this policy option the application of the *lex specialis* principle would be clarified. In particular, the amended NIS Directive would establish that, in order to contribute to the uniform applicability of this provision, the Commission may adopt guidelines.

More coherence would be achieved between the NIS requirements and the cybersecurity requirements concerning **providers of electronic communications networks or of publicly available electronic communications services**. The NIS Directive excludes from its security and notification requirements these providers. The cybersecurity aspects in relation to these services are regulated, starting December 2020, by the European Electronic Communications Code (EECC). Seven Member States added these services to the scope of the NIS-related rules. An online survey conducted by ENISA in mid-2020 addressed the issue of the effectiveness of telecom security legislation.<sup>158</sup> The vast majority of respondents found that the EU telecom security legislation is not consistent with the NIS Directive, that the national capabilities on telecom security are not comparable across the EU and that technically the telecom security requirements are not similar across the EU.

#### ***Option 3: Systemic and structural changes to the NIS Directive (new directive)***

This scenario would entail systemic and structural changes to the NIS Directive (through a new directive) envisaging a more fundamental shift of approach towards covering a wider segment of the economies across the Union, yet with a more focused supervision targeting big and key players. It would also streamline the obligations imposed on businesses and ensure a higher level of harmonisation thereof, create a more effective setting for operational aspects, as well as establish a clear basis for enhanced shared responsibilities and accountability of various stakeholders on cybersecurity measures.

In particular, the following measures are envisaged:

#### ***1. Sectoral scope and coverage of entities***

**Additional sectors, subsectors and types of services** would be brought under the NIS **scope**, enlarging the fraction of economy covered by the NIS framework, same as described above under option 2. The list of sectors and services falling within the NIS scope would form part of the revised NIS Directive and can only be supplemented or changed by another legislative amendment or review.

As regards the **entities** active in the sectors, subsectors and types of services falling within the NIS scope, option 3, unlike option 2, would define a clear-cut NIS scope, and consequently the requirements stemming from that, focusing on big and key entities, yet essential and important for the Member States' economies and societies. This would allow a reallocation of resources for competent authorities to focus on a more pro-active approach, monitoring and analysis of new threats, supervisory measures, providing support to businesses. This option would also introduce a differentiation among entities based on importance and/or criticality, as well as a size cap, to ensure a targeted and well-defined NIS scope. More clarity and certainty would have a high potential to ensure

---

<sup>158</sup> The respondents to the survey were 27 stakeholders from national telecom security authorities, NIS competent authorities or CSIRTs, providers of electronic communications networks or services, telecom equipment suppliers or vendors, as well as others.

a good compliance rate, incentivise cybersecurity investments and foster trust and cooperation. These would be achieved as follows:

- ✓ The entities falling within the NIS scope would **no longer be distinguished on the grounds of being operators within an essential sector or a digital service provider**, as this categorisation has proven obsolete. In practice, OESs are dependent on certain digital service providers, such as cloud service providers, which makes the latter as important or essential as the former and hence requires a similar regulatory regime. Instead, entities would be **classified in two categories (i.e. essential and important)**, depending on their **importance and/or criticality**.
- ✓ The revised NIS Directive would provide for a list of sectors and types of services where the entities falling within the NIS scope would be ‘essential’, and a respective list of sectors and types of services for ‘important’ entities. ‘Important’ entities, as opposed to ‘essential’ would be active in sectors, subsectors or provide services which are considered of importance for economies and societies, yet not as vital as those in the ‘essential’ category. This categorisation takes account of the level of criticality of the sector or type of service, and notably the level of dependency of other sectors or types of services or interconnectedness between sectors. The entities under the NIS scope operating in the sectors which are currently qualified as ‘essential’ would by default be considered ‘essential’ in the new NIS framework.
- ✓ Both essential and important entities would be subject to the **same security requirements and reporting obligations**. At the same time, this categorisation would ensure a fair balance for both competent authorities and entities between requirements and obligations on one hand, and the administrative burden stemming from the supervision of compliance on the other hand. This balance should be guaranteed through a **differentiation in the supervisory and penalty regimes** between these two categories of entities. More specifically: essential entities should be subject to a fully-fledged supervision, both *ex-ante* and *ex-post*, while the important entities would be subject only to *ex-post* supervision (i.e. reactive and without a general obligation to systematically document compliance).

Table 4 below lists **all sectors and services for essential and important entities falling within the NIS scope**, as it would be provided by the revised NIS Directive in option 3.

<i>Sectors, subsectors and types of services defined by the NIS scope for <u>essential</u> entities</i>		<i>Sectors, subsectors and types of services defined by the NIS scope for <u>important</u> entities</i>
Energy	Electricity (generation, supply, distribution, transmission, nominated electricity market operators, electricity market operators providing aggregation, demand response or energy storage services)	Food supply <sup>159</sup>
	Oil (including central oil stocking entities)	

<sup>159</sup> This is complemented by production and processing covered under the manufacturing sector.

	Gas		
	Operators of hydrogen production, storage and transmission		
Heat production and supply		Waste management	
Transport	Air	Postal and courier services	
	Rail		
	Water		
	Road		
Banking		Manufacturing (certain subsectors) <sup>160</sup>	
Financial market infrastructures		Chemicals ( <i>manufacture, production and distribution</i> )	
Health	Healthcare providers	Digital services	Online marketplaces
	EU reference laboratories		Online search engines
	Entities conducting research and development activities of medicinal products		Social networks
	Entities manufacturing basic pharmaceutical products and pharmaceutical preparations <sup>161</sup>		
	Entities manufacturing medical devices considered as critical during a public health emergency <sup>162</sup>		

<sup>160</sup> As described under option 2, Table 3, footnote 137.

<sup>161</sup> Undertakings carrying out the manufacture, production and distribution of substances and articles as defined in points (4), (9) and (14) of Article 3 of Regulation (EC) No 1907/2006.

<sup>162</sup> According to Article 20 of the Commission Proposal for a [Regulation on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (COM92020)725 final).

Wastewater systems		
Drinking water distribution and supply		
Digital infrastructure	IXP providers	
	DNS service providers <sup>163</sup>	
	TLD name registers	
	Cloud computing services	
	Trust service providers	
	Data centres	
	Content Delivery Network providers	
Providers of electronic communications networks or of publicly available electronic communications services <sup>164</sup>		
Public administration <sup>165</sup>		
Operators of government-owned and privately-owned ground-based infrastructure that support the provision of space-based services		

**Table 4:** sectors, subsectors and services that would fall within the NIS scope under policy option 3

- ✓ The **identification system for OES** would be **replaced by uniform criteria for all entities** (both essential and important): i.e. a **size-cap rule**<sup>166</sup> would be introduced

<sup>163</sup> The definition would be further clarified, as mentioned in option 2.

<sup>164</sup> As in the option 2, the respective provisions of the EECC would be repealed.

<sup>165</sup> As defined in option 2.

<sup>166</sup> Medium and large size enterprises as defined by the new NIS legal framework, based on number of employees and turnover, according with Commission Recommendation 2003/361/EC of 6 May 2003. In particular, the category of medium enterprises is made of enterprises which employ between 50 and 250 persons and which have the annual turnover and/or annual balance sheet total between EUR 10 million and 50 million EUR (or, in the case of the balance sheets, up to EUR 43 million). The category of large enterprises is made of enterprises which employ over 250 persons and which have an annual turnover exceeding 50 million EUR and/or annual balance sheet total exceeding EUR 43 million.

establishing that all medium and large entities<sup>167</sup> active in the (sub)sectors and services covered by the NIS framework would automatically fall within the NIS scope. **Small and micro enterprises would therefore be excluded from the scope.** Member States would not be required to establish a list of the entities that meet this generally applicable size-related criterion, but they may choose to do so in order to facilitate interactions with the entities in scope and supervision.

- ✓ While the size-related criterion is not necessarily an ideal stand-alone criterion to determine the importance and/or criticality of an entity, it is nevertheless a meaningful proxy for determining whether entities play a key role for society and economies. Moreover, its aim would be to set a clear-cut directly applicable criterion to avoid the complexity that other types of criteria or combination thereof, such as number of users relying on a service, dependency on other sectors or maintaining a sufficient level of service, generated in the implementation of the NIS Directive. All entities fulfilling these criteria would be by default subject to the requirements set out by the NIS framework. 67% of the competent authorities responding to the NIS review study survey considered that the general obligation for all entities above a certain size to implement security requirements and report incidents could improve the current identification system.
- ✓ In the early stages of the NIS review process, the **alternative of setting up of harmonised sector-specific thresholds** was considered. Such alternative was however considered not viable and discarded at an early stage. This is because it would be partially perpetuating the status quo, where Member States establish their own thresholds for the identification of operators of essential services, many of which are sector-based. Such an alternative would not be compatible with the discarding of the current complex identification process and would likely lead to lengthy negotiations on thresholds where the views may differ considerably among Member States.
- ✓ In order to ensure that small or micro entities which are nevertheless of critical importance for the societal or economic activities are not left out of the NIS scope, **exceptions to the size-cap rule** would be established. These would be as follows: (i) absence of alternative service providers in a Member State (i.e. operators that are the sole providers of a service in a given Member State), (ii) the impact that a potential disruption could have on public safety, security or health<sup>168</sup>, (iii) Member States would be allowed to include in the NIS scope micro or small entities active in the sectors and services covered by the NIS framework justified on the basis of their specific importance at regional or national level for that particular sector or type of service or for other interdependent sectors or services, (iv) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact, (v) the entity is identified as a critical entity or as an entity equivalent to a critical entity in accordance with the Directive on the resilience of critical entities. Member States would be responsible for determining which small or micro entities meet these criteria and submit to the Commission the lists of such entities every two years. The Commission may adopt guidelines, in cooperation with the Cooperation Group, on the application of the above-mentioned criteria for exceptions to the size-cap rule. Furthermore, operators and providers of electronic communications networks and

---

<sup>167</sup> As defined by the Commission Recommendation 2003/361/EC of 6 May 2003.

<sup>168</sup> Term to be defined in the new NIS directive that would nevertheless imply a certain analysis from the national competent authorities on a case by case basis.

services or the trust service providers would be excluded from the size cap rule, given that these entities, including micro and small, are already applying high standard cybersecurity measures according to their respective regulations.<sup>169</sup> Top-level domain name registries and domain name system (DNS) service providers would also be excluded from the size-cap rule.

- ✓ In order to ensure a clear overview of **all essential and important entities providing digital services of cross-border nature**, ENISA would **hold a registry** thereof. The entities in question would be under the obligation to notify themselves to ENISA following a clear template or, alternatively, ENISA could establish the registry based on own research and/or in cooperation with the competent authorities. This option is therefore expected to lead to a more conclusive overview of the digital services, also because it would allow a more effective supervisory regime, while also better considering the interdependencies between OESs and DSPs.

In this policy option, **the number and extent of coverage** of the **entities active in the sectors, subsectors and services** currently covered by the NIS Directive would indeed increase as compared to the current OES identification-based system. However, the application of the size-cap rule would ensure a focus on a number of companies which could be subjected to effective supervision and prioritisation by competent authorities. This would concern:

- 3,099 companies for **electricity and gas supply**<sup>170</sup>, 380 for **water transport**, 228 for **air transport**, 450 for **rail transport**, 870 for **water collection, treatment and supply**.
- For **banking and financial market infrastructure**, the number of entities that would be covered by default would be higher in particular for banking (6,088 banks, of which approx. 3,500 medium and large) and less considerable for financial market infrastructures (350 entities, as compared to 172 OES identified). However, the banking and financial market infrastructure sectors would be covered in the future as *lex specialis* by the DORA.
- In the **health** sector, estimates indicate approximately 13,200 hospitals in Europe<sup>171</sup>. There are no available data on the number of medium and large hospitals. The total number of hospitals cannot however be compared with the number of currently identified OESs in the healthcare system (i.e.12,469). This is because about 87% of the number of identified OESs comes from the same Member State which identified every single healthcare provider<sup>172</sup> in the country, no matter the size, thus illustrating once more the deep divergence in the identification approaches at Member States level. In option 3, with the application of the size cap, this number is expected to considerably decrease. At the same time, additional medium and large hospitals in other Member States that currently were not identified as OES would be added to the NIS scope. The overall resulting number is however expected to be lower than the couple of thousand ranges.

---

<sup>169</sup> i.e. the European Electronic Communications Code (Articles 40 and 41) and the eIDAS Regulation (Article 19).

<sup>170</sup> To note that these aggregate data also include energy generation companies, which are currently not in the NIS scope and are considered under policy options 2 and 3.

<sup>171</sup> 2.6 hospitals for 100,000 inhabitants estimated in Europe in 2015: <https://hospitalhealthcare.com/latest-issue-2018/hope-2018/hospitals-in-europe-healthcare-data-9/>

<sup>172</sup> hospitals and doctors' cabinets.

- For **digital infrastructure**, options 3 does not appear to bring considerable changes in terms of coverage of entities. In particular, 173 such entities were identified as OES by the Member States, while there are: 28 major country-code top-level domain (ccTLD)<sup>173</sup>; 140 IXPs<sup>174</sup> (with one company usually administering several IXPs); for authoritative DNS resolution: two root name servers<sup>175</sup>, 28 major ccTLD entities<sup>176</sup> and a large number of domain name registrars and web hosting companies<sup>177</sup>, and for recursive DNS resolution: DNS resolvers provided by most internet service providers<sup>178</sup> and by third parties, mostly large global technology companies located outside the EU.
- ✓ As regards **digital service providers**, the changes brought by policy options 2 and 3 would not be that significant in terms of scope of entities. This is notably given that the size cap rule already applies to these providers in line with the current NIS Directive.
  - For **online search engines**, the market in Europe is dominated by one player, Google, which has over 90% of the general search market in Europe<sup>179</sup>, followed at a big distance (i.e. less than 3% share of general search market) by Bing and few European-based companies, such as Seznam in Czechia or Qwant in France.
  - For **online marketplaces**, certain estimates indicate about 7,000 marketplaces in Europe<sup>180</sup>, yet the number of medium and large marketplaces that would be covered in option 3 was estimated at a much lower level, i.e. about 120.<sup>181</sup>
  - According to the 2020 Digital Economy and Society Index (DESI)<sup>182</sup>, in 2018, 26% of European enterprises purchased **cloud computing services** and incorporated cloud technologies. Among the enterprises that used cloud computing services, 55 % were ‘highly dependent’.<sup>183</sup> Some estimates indicate about 1,700<sup>184</sup> cloud service providers in Europe. Overall, there are only few large companies on the European market: Amazon<sup>185</sup>, Microsoft, Google and

<sup>173</sup> one in each Member State plus EURid, which administers .eu

<sup>174</sup> Referenced for 2020. The 140 IXPs are located in the EU, with some being of global importance.

<sup>175</sup> providing authoritative DNS resolution for the root zone, located in the Netherlands and Sweden.

<sup>176</sup> The ccTLDs of the 27 Member States (such as .de, .fr or .pl) and of the European Union (.eu), but not counting regional ccTLDs, such as .ax of Åland Islands (Finland). These provide authoritative DNS resolution for their respective TLD namespaces.

<sup>177</sup> offering authoritative DNS resolution as part of their domain registration services.

<sup>178</sup> As part of the internet access arrangement. See the data on electronic communication networks and services.

<sup>179</sup> Netmarketshare.com.

<sup>180</sup> Commission estimate of 2019: [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_1168](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168)

<sup>181</sup> Conservative estimate based on a sample of marketplaces for a competition-related sector inquiry conducted by the Commission in 2015-2017: REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report on the E-commerce Sector Inquiry, COM(2017) 229 final and SWD(2017) 154 final: [https://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_sw\\_d\\_en.pdf](https://ec.europa.eu/competition/antitrust/sector_inquiry_sw_d_en.pdf)

<sup>182</sup> <https://ec.europa.eu/digital-single-market/en/integration-digital-technology>

<sup>183</sup> At the two extremes, the majority of enterprises in the manufacturing sector (51 %) belonged to the upper-medium dependence group, while the majority in information and communication (71 %) reported using advanced services and hence belonged to the high dependence group.

<sup>184</sup> There is no precise estimate of the number of European cloud service providers, only estimates such as this one by business information platforms: <https://www.crunchbase.com/hub/europe-cloud-computing-companies>

<sup>185</sup> Biggest player in France, Germany, the UK and the Netherlands.

IBM.<sup>186</sup> OVH (the largest European Cloud Service Provider) gets less than 1% of total revenues generated in this market.

As regards the **entities active in the new sectors, subsectors and services** considered in this option:

- ✓ For **providers of electronic communications networks or of publicly available electronic communications services**<sup>187</sup>, this option would cover all entities, irrespective of the size. This represents an exemption from the size cap rule, due to the fact that it is a highly regulated sector, now through the European Electronic Communication Code, already implementing a high level of security standards. Excluding micro and small providers from the NIS scope may negatively impact these existing standards. Given that the level of cybersecurity capabilities of these entities is expected to be rather high already, including on documentation of compliance with security requirements, the supervision is not expected to bring a notable burden to the competent authorities. Similarly, trust service providers would be exempted from the size cap rule, given that within the eIDAS framework, some security standards are already implemented; indeed, excluding micro and small providers from the NIS scope may negatively impact these existing standards.
- ✓ For new sectors considered, the number of entities (medium and large) concerned by this policy option 3 would be as follows: i.e. for **manufacture of chemicals and chemical products**: 3,193 companies; for **waste management** (waste collection, treatment and disposal activities): 2,616 medium and large companies; for **wastewater** (sewerage): 473 medium and large companies; for **postal and courier services**, 869 medium and large companies; for **food supply**<sup>188</sup>: 5,303 medium and large companies; for **manufacturing, for 8 selected subsectors** (other than chemicals)<sup>189</sup>: 30,942 medium and large companies. For these new sectors, even with the application of the size cap rule, would determine competent authorities to establish supervisory strategies and prioritise supervision activities.
- ✓ As regards **energy subsectors, data centres, content delivery networks and social networks**, the data presented and explained under policy option 2 would also be applicable here.

## 2. *Security requirements and reporting obligations*

Uniform **security requirements** and **incident reporting obligations** for all essential and important entities would be established, same as in option 2. Furthermore, as in option 2, the Commission would be empowered to issue delegated acts for specifying and supplementing the elements established by the NIS framework. In addition:

- ✓ As **part of the security requirements**, in particular the risk assessment obligations, entities would need to demonstrate how they assessed *supplier-specific risks* and how they have mitigated them. This would include security elements concerning supplier relationships, including providers of data storage and processing services. Entities would therefore be asked to assess and take into account the overall quality of

---

<sup>186</sup> Salesforce, Rackspace and Oracle are global providers that are further down in the country rankings, with Salesforce ranking fifth overall across Europe. European players such as OVH, Enter, Aruba, Outscale and Fabasoft do not grasp any significant market shares globally.

<sup>187</sup> Broadcasting services and emergency communication services are also considered under this sector.

<sup>188</sup> The data represent an overestimate, since they also cover wholesale and retail of tobacco, which would not be included in the NIS scope in policy options 2 and 3.

<sup>189</sup> food products; beverages; basic pharmaceutical products and pharmaceutical preparations; computer, electronic and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers and semi-trailers; other transport equipment.



products and cybersecurity practices of their suppliers and service providers. This could be documented by results of checks and audits. To assist entities to appropriately manage supply chain and supplier-related cybersecurity risks, the Commission, in cooperation with the Cooperation Group and ENISA, would carry out sectoral supply chain risk assessments with the aim of identifying per sector which are the critical ICT services, systems or products, relevant threats and vulnerabilities. Based on this analysis, the Commission may issue recommendations on how these risks could be addressed.

- ✓ An obligation would be introduced for SPOCs to provide a **monthly summary incident report to ENISA**, including anonymised and aggregated data on cybersecurity incidents, near misses, significant cyber threats and vulnerabilities. The monthly reporting of summary of incidents, significant cyber threats and vulnerabilities by the SPOCs would not be expected to impose a notable burden on the latter since they would pass on readily available data in an anonymised aggregated format, while at the same time a monthly input to ENISA would allow a timely assessment of taxonomy of incidents and level of threats; this would facilitate timely information sharing across Member States. ENISA would also provide technical guidance for such reporting.
- ✓ A new rule would be introduced to **simplify** the compliance burden for entities falling under the scope of other EU legislation in terms incident reporting. Depending on whether personal data is compromised or not and whether a data breach poses a risk to the fundamental rights and freedoms of the natural persons, a security incident under the NIS Directive might trigger additional reporting obligations for the entities under another EU legislation (i.e. under the GDPR or the ePrivacy Directive). This multiple reporting is perceived as an unnecessary compliance burden for all entities concerned. In order to simplify the process and release the companies from this excessive burden, the revised NIS Directive would encourage Member States to create a **single entry point for notifications concerning security breaches stemming from the NIS Directive**, the General Data Protection Regulation and the ePrivacy Directive. In addition, ENISA, in cooperation with the NIS Cooperation Group and the Commission, would develop common templates by means of guidelines that would simplify and streamline the reporting information requested by the different EU legislations.

In this policy option, the **alternative** of imposing a centralised reporting obligation for entities at European level was not considered viable. This is mainly because it would have put a disproportionate burden on companies, which would have had to report incidents at both national and European levels, while the technical aspects of setting up such a system and its potential to lead to effective results and ultimately an improvement of the cyber resilience levels for companies across the Member States were unclear.

As regards the **Member States' capabilities**, this option would reinforce the active role of competent authorities and CSIRTs, which may trigger a prioritisation of resources at national level.

### ***3. Supervision and enforcement***

This option would put supervision at the heart of the tasks of the competent authorities and set a coherent framework for all supervisory activities across Member States. Moreover, a minimum list of sanctions for breach of the NIS obligations would be provided, setting a clear consistent framework for sanctions across the Union. A minimum for the maximum level of administrative fines linked to the turnover is expected to further ensure dissuasiveness. A rule of liability of natural persons holding

representation positions/roles would also be introduced to ensure real accountability for cybersecurity policies at organisational level. A strengthened supervision and enforcement framework, setting up certain minimum requirements, may lead to better reporting of incident rates that could also have an impact of detection of data breaches.

- ✓ On **supervision**, the revised NIS Directive would provide for a minimum list of *ex ante* and *ex post* supervisory actions and means through which competent authorities could exercise their supervisory powers (e.g. conduct and/or order regular and targeted audits, on-site and off-site checks, type of evidence and information the entities are bound to provide upon request). In addition, there would be a **differentiation of supervisory regime between essential and important entities**. Thus, essential entities will be subject to a fully-fledged supervisory regime (*ex-ante* and *ex-post*), while important entities will only be subject to a light supervisory regime, *ex post* only, which would put less burden on both companies and competent authorities. For the latter, this would mean that important entities would not have to systematically document compliance with the security requirements, while competent authorities would implement a reactive *ex post* approach to supervision<sup>190</sup> and hence would not have a general obligation to supervise these entities.
- ✓ On **enforcement**, in addition to what is envisaged by option 2, the new NIS legal act would establish a list of administrative sanctions (e.g. binding instructions, order to implement the recommendations of a security audit, designation of a monitoring officer, administrative fines), that Member States should provide for in national law.<sup>191</sup> In terms of type of applicable **penalties**, the new NIS legal act would set the Member States' obligation to provide for administrative fines<sup>192</sup> among the applicable sanctions for essential entities, with a maximum of at least 10,000,000 EUR or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.<sup>193</sup> The revised NIS Directive would also require Member States to take account of the particular circumstances of each case when triggering liability and applying sanctions for non-compliance (e.g. the seriousness and duration of the infringement, the intentional or negligent character of the infringement, the actual damage caused, the preventive measures put in place to mitigate the damage, the level of cooperation with the competent authorities, etc.)
- ✓ In relation to entities which are not established in the Union, but provide services in the Union, the revised NIS Directive would clarify that any Member State in which the entity provides services may take legal actions against the entity for non-compliance with its NIS-related obligations.
- ✓ The **liability of the natural person(s) responsible for or acting as a representative of the legal person** for potential violations of the NIS legal framework would be introduced.

---

<sup>190</sup> As explained in section 1.1., with this approach, DSPs do not have to gather evidence on the implementation of security policies and the competent authorities should have no general obligation to supervise DSPs, thus discouraging a pro-active approach from the latter.

<sup>191</sup> e.g. issue binding instructions or an order to remedy the deficiencies, order to implement the recommendations of a security audit, designate a monitoring officer, impose or request the imposition of administrative fines, etc.

<sup>192</sup> The harmonised level of minimum administrative fines considered the newest legislative trends in some Member States and the provisions of related EU legislation, notably GDPR.

<sup>193</sup> where the legal system of the Member State does not provide for administrative fines, the respective provisions may be applied in such a manner that the fine is initiated by the competent authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by competent authorities.

In this option, unlike policy option 2, the more prescriptive approach towards supervision and enforcement is matched by the clear-cut scope by sectors and entities established by the revised NIS Directive and through a generally applicable rule. However, the **alternative** of establishing a centralised European supervision system was considered non-viable for the NIS framework, as it would have been disproportionate and would not have allowed Member States to adapt the supervision to their national context and legal order.

A **peer review mechanism** would be introduced, allowing the assessment by experts designated by the Member States of the implementation of cybersecurity policies, including the level of Member States' capabilities and available **resources**.<sup>194</sup> The peer-review findings would not be binding on the Member States. An **alternative** considering mandatory conclusions of the peer-reviews would go counter to the nature of the mechanism which aims at gradually building trust and encouraging exchanges of practices and well-informed advice among Member States.

This option has potential to contribute more visibly to improving and levelling the Member States' **capabilities**, mainly through the peer-review and the mutual assistance mechanisms, which could ensure peer pressure for a comparable level of financial, technical and human resources across Member States.

#### ***4. Cooperation and information sharing***

In this option, a clear-cut mandatory mutual assistance mechanism would be set up for cross-border cases. The observatory role of ENISA for the state of cybersecurity in the Union would be enhanced, expected to help bringing together the capabilities of Member States and creating the premise for enhanced information sharing among Member States. The Cooperation Group would organise regular joint meetings with various stakeholders, including businesses, to exchange views and gather relevant input on emerging policy challenges in the area of cybersecurity. In option 3, the introduction of a cybersecurity crisis management framework would institutionalise the existing efforts for operational cooperation in times of crisis. More specifically:

- ✓ As regards **cross-border** cooperation and information sharing for **competent authorities and private actors**, in option 3, the new legal act, in addition to what was described in option 2, would:
  - introduce provisions on cross-border cooperation and mutual assistance (including on cross-border dependencies) and notably: (i) information sharing and consultation on supervisory and enforcement measures; (ii) possibility of a Member State requesting supervision in another Member State; (iii) obligation of a Member State to provide cross-border assistance to another Member State; (iv) voluntary joint supervisory action.
  - require Member States to develop a common policy framework on **co-ordinated vulnerability disclosure** and designate a national CSIRT as a coordinator and facilitator at national level. ENISA would maintain a registry for all notified newly discovered vulnerabilities with their characteristics.

---

<sup>194</sup> The reviews shall be conducted by cybersecurity experts coming from different Member States than the one reviewed and shall cover at least the following aspects: (i) the effectiveness of the implementation of the security requirements and reporting obligations; (ii) the level of capabilities, including the available financial, technical and human resources, and the effectiveness of the exercise of the powers pertaining to national competent authorities; (iii) the operational capabilities and effectiveness of CSIRTs; (iv) the effectiveness of cross-border cooperation; (v) the effectiveness of the information-sharing framework.

- require Member States to develop a common policy framework addressing the cybersecurity in the **supply chain** for components used by essential entities, including the development of an assistance mechanism for the purchase of cybersecurity solutions by public buyers.
- ✓ A more operational-oriented approach would be introduced to include specific provisions on **crisis management at both national and EU level**. Indeed, a cybersecurity crisis management framework would be built in the NIS framework. At national level, Member States would be required to designate competent authorities, set out specific plans and identify national capabilities, assets and procedures that can be deployed in case of cross-border cyber crisis. At EU level: CyCLONe', stemming from the application of the Blueprint Recommendation, would be institutionalised. An EU cybersecurity crisis management framework, incorporating CyCLONe for the operational exchanges, would be established.
- ✓ ENISA, with support from the Commission, would act as an **observatory of the state of cybersecurity in the Union**. This may entail, among others: (i) gathering regularly relevant data and information; (ii) publishing, with support from the Commission, a regular report (biennial) on the state of cybersecurity in the EU; (iii) establishing and holding a cybersecurity index.

##### 5. Synergies with other related instruments

This option is expected to ensure further coherence with other legal instruments, notably given the additional clarifications of certain principles and legal concepts, in combination with the extension of the scope of application and the focus on key entities. As in option 2, this policy option would also bring clarifications to the application of the *lex specialis* principle and it would bring under the scope of the NIS Directive the trust service providers and the providers of electronic communications networks or of publicly available electronic communications services, thus ensuring simplification and more coherence. The revised NIS framework in all policy options would also observe implementing powers that have been conferred to the Commission and which could be used to specify sectoral cybersecurity requirements.

Considering the wide sectoral scope, combined with streamlined security requirements and a more effective supervision system, the likelihood of the need to establish other potential cybersecurity requirements in sector-specific instruments is expected to be slightly reduced as compared to the other policy options.

As regards the synergies with the **review of the ECI framework**, as explained under the baseline scenario, this would set out minimum requirements to address non-cyber threats for operators defined as critical. This approach is also maintained with the introduction of 'essential' and 'important' differentiation among NIS entities. Furthermore, in this policy option, Member States would be required to ensure that their cybersecurity strategies provide for a policy framework for enhanced coordination between the competent authority under the NIS Directive and the Directive on the resilience of critical entities in the context of information sharing on incidents and cyber threats and the exercise of supervisory tasks. Moreover, in order to promote strategic cooperation and exchange of information at a Union level, this policy option would establish that the NIS Cooperation Group would meet on a regular basis and at least once a year with the cooperation body under the Directive on the resilience of critical entities, the Critical Entities Resilience Group.

## 6.2. Options discarded at an early stage

### *Option 1: Non-legislative measures to align the transposition of the NIS Directive*

This option was discarded at an early stage, on the grounds that it would not substantially differ from the status quo. The only notable difference would consist of the use of the Commission's incentivizing and guiding role through the issuing of guidelines and/or recommendations on some of the most problematic issues that have met a divergent implementation so far and led to fragmented approaches.

However, the same 'soft' outcome would most likely be ensured by further guidance issued by the Cooperation Group within its existing mandate. The guidance and reference documents that the Cooperation Group issued so far on some of these matters that encountered divergent practices (e.g. OES identification, incident notification, security requirements for OES) did not prove sufficient to address the most serious discrepancies in the implementation of the NIS Directive. Furthermore, the Cooperation Group has already issued reference documents on aspects such as the consultation process in cases with cross-border impact.<sup>195</sup> However, this did not lead to an increase in the number of such cross-border consultations (*section 2.1.3*). The Commission also formulated recommendations in its 2019 Report on the identification of OES. However, these have not generated any significant change in the direction of further alignment of approaches or a more conclusive coverage of OESs across Member States. (*section 2.2.2*.)

Furthermore, ENISA continues to develop guidelines and make good practice known on a wide range of technical aspects. In the current setting, the Commission may also develop and publish recommendations, reports and guiding principles, following consultation with relevant stakeholders.

Overall, the consultations held as part of the NIS review process, including the results of the targeted surveys of the NIS review study, as well as the open public consultation, have shown that all relevant categories of stakeholders support a change in the status quo on key aspects of the NIS Directive, such as the OES identification process or incident notifications, which would require legislative solutions. For example, a significant share of the OPC respondents found that the current NIS Directive's approach does not ensure that all relevant OESs are identified across the Union (37.4% disagreed and 6.3% strongly disagreed). In relation to incident notifications, 56% of the competent authorities and 53% of the OESs responding to the NIS review study survey considered to a great or moderate extent that the notification obligations should be better streamlined. *See Annex 6 for a selection of the results of the targeted surveys and Annex 2 for the OPC results.*

In addition, as highlighted in *section 6.2.*, a number of potential **alternatives to various areas of intervention** within the policy options have been discarded at an early stage and considered non-viable.

***Complementarity between the NIS review and the review of the framework for the European critical infrastructure:*** The Commission is also preparing, in synergy with the review of the NIS Directive, a review of the Directive on the identification and designation of **European critical infrastructures**<sup>196</sup> (hereinafter called 'the ECI Directive'), with a view to adopt a proposal by the end of 2020. The aim of the latter is to

---

<sup>195</sup> *Identification of Operators of Essential Services - Reference document on modalities of the consultation process in cases with cross-border impact*, available here: <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

<sup>196</sup> Council 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, OJ L 345, 23.12.2008, p. 75–82.

enhance the physical protection and resilience of critical infrastructure against threats such as terrorism or natural disasters. Even if the two initiatives are complementary, in the NIS review context the option of addressing the resilience of critical (physical) infrastructures and that of the network and information systems underpinning essential services in a single legislative framework, was not considered. This is because the nature, material scope and specific objectives of the two initiatives are different. The NIS framework focuses on cybersecurity aspects, covering a wide sectoral base, including also digital services. The ECI framework aims at ensuring a more targeted cross-sector protection mainly focused on responding to non-cyber risks. Furthermore, unlike cybersecurity requirements, the security requirements for critical infrastructures in terms of non-cyber threats have to remain general in nature. This is because security measures are to be defined by the operators themselves –with the support and oversight of relevant authorities, to reflect the specificities related to the type of infrastructure, its location or the relevant threats.

## 7. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

This section analyses the economic, environmental and social impact of the options, as well as their effectiveness vis-à-vis the specific objectives set out in *section 5.2.*, in line with the Better Regulation Guidelines, together with the coherence with other policies and the views of stakeholders.

### 7.1. Economic impact and efficiency

#### Private sector/industry

In order to determine the potential impact of the policy options on businesses, the impact assessment considered the following steps: (i) determining the coverage of the entities active in the current and future sectors, subsectors and types of services that would fall within the NIS scope in policy options 2 and 3; (ii) estimating the average costs calculated as percentage of ICT security spending out of ICT spending and total revenue per sector and the likely evolution thereof; (iii) estimating costs and benefits at the level of organisations. The particular economic impact on SMEs is also being analysed.

There are currently no available data comparable across the EU to measure the return of security investment (ROSI) at the level of companies across sectors or per sector. While there are some models for the calculation of the returns of investment and in particular security metrics or cyber threat metrics, there is an overall absence of consistent data based on real cases that could support such metrics.<sup>197</sup> This is acknowledged by further research.<sup>198</sup> The ROSI model finds that the optimal level of security is reached when the cost of security measures equals the costs of security breaches.<sup>199</sup>

---

<sup>197</sup> When it comes to cybersecurity metrics, although there appears to be a wealth of such metrics, some listing hundreds, ‘*challenges still remain in the calculation of proper values of risk metric variables. [...] At the moment, companies use different techniques to evaluate internal costs arising from security incidents. [...]*’ Furthermore, network externalities and security interdependency renders this task even more difficult. In the same vein, the July 2020 JRC Report ‘*Cybersecurity – Our Digital Anchor*’ states that, ‘*while organisations invest a lot of money and human capital in enforcing and strengthening their cybersecurity, there is still no globally accepted and standardised way of measuring it. According to a 2019 Court of Auditors’ report, this makes it difficult to decide which investments have resulted in a safer organisation. [...]*’

<sup>198</sup> *Security Metrics and Security Investment Models*, Rainer Boehme, International Computer Science Institute, Berkeley, California, USA;

<sup>199</sup> The report of March 2015 on the ‘*State-of-the-art of the Economics of Cyber-security and Privacy: IPACSO – A Coordination Action under the FP7 DG CNECT Trustworthy ICT Program, deliverable D4.1; delivered in the context of the EU-funded Coordination and Support Action (CSA) project aimed at supporting Privacy and Cyber-security innovations in Europe.*’

As stressed by the IPACSO report, the main objective of **cybersecurity investments** is to reduce the risk of security breaches, while at the same time reducing in variability of potential losses from cybercrime. In this context, the limited information available on estimated cost-benefits, trade-offs and the budgetary constraints often have negative effects on the decision to invest more at the level of an organisation. At the same time, literature has shown that cybersecurity investments are primarily of cost-saving nature as compared to other measures that improve revenues.<sup>200</sup> Research indicated that companies **often rely on reactive investment strategies** when it comes to cybersecurity rather than proactive, as it is often more efficient to rely on proven existing technologies and be able to quickly implement patches and beef up security after breaches occurred.<sup>201</sup>

The IPACSO report points to the following typical costs and benefits, while stressing that the tangible benefits of cybersecurity investment are very difficult to estimate.

- *Costs*: personnel costs (e.g. set up of new in-house teams), purchase cost (hardware, software, consultancy services), administrative costs, opportunity costs, in-house R&D.
- *Benefits*: decrease in security incidents & cybercrime losses; reduction in costs of liability for breaches; increase in trust of customers; increase in company reputation; protection from unfair competition (industrial espionage); reduction in switching of disgruntled customers to competitors; increase in compliance.

The analysis below would therefore consider these typical costs and benefits. There is no available comparable economic data to measure the actual impact of the NIS Directive on the costs and benefits of the companies active in the sectors and subsectors or providing services under the NIS scope<sup>202</sup>. Given these lacunae, the analyses of economic impact and efficiency under all policy options, including the baseline scenario, would refer to widely accepted qualitative indicators for assessing the costs and benefits of various cybersecurity measures, along the lines described above, quantitative estimates or assumptions, and information gathered through the NIS review country visits or the consultations held in this process with the relevant stakeholders.<sup>203</sup>

- *Coverage of the entities active in the current and future sectors, subsectors and types of services that would fall within the NIS scope*

In option 3, approx. 110,000 entities (i.e. medium and large) would be covered under the NIS scope (i.e. summing up the available data provided in *Annex 3, tables 1 and 2*). Of these, based on the available data detailed in *Annex 3*, approx. 67,000 would be essential entities and approx. 43,000 important entities. In option 2, while no size filter would be

---

<sup>200</sup> An additional challenge are the direct and indirect costs entailed by cybersecurity expenditure. The direct costs and benefits concern the company which makes the cybersecurity investment as such, while the indirect costs and benefits concern other market players, for example, in the value chain, the investment of a company in a secure system indirectly affects positively the security of other connected companies and services (network externalities).

<sup>201</sup> IPACSO Report, page 12, reference to a study of the Research Triangle Institute in 2006 in the US.

<sup>202</sup> An ongoing study commissioned by ENISA and implemented by Gartner aims at providing such specific costs and benefits estimates corresponding to the impact of the NIS Directive. The first preliminary results of this study are expected to be published in December 2020.

<sup>203</sup> While the overall methodological approach of the EU Standard Cost Model set out by the Better Regulation tools was taken into account in the assessment of costs and benefits, it was not possible to provide precise estimates per organisation of a level of granularity going up to precise price per action, value of additional equipment needed, costs of outsourced services, etc. The analysis below provides average cross-sector estimates, notably linked to estimates of average ICT security spending and FTEs. More granular estimates are possible due to the considerable cross-sector and cross-sector differences, as well as in the level of cybersecurity maturity and resources of organisations.

applied, the identification process will be maintained, hence the Member States will retain the discretion to identify the operators of essential services falling within the NIS scope. In options 0 and 1, the number of OESs is not expected to considerably increase from today (i.e. 15,519 based on the Member States' notifications until the beginning of October 2020). Updated notifications are currently being submitted by the Member States to the Commission<sup>204</sup>, indicating a potential increase of the overall number of OESs from 2018 until end 2020 of approximately 3,600 OES.

- ***Estimated cumulated costs of the policy options translated in the overall level of ICT security spending and investment – i.e. impacts triggered by the NIS scope***

The level of **investment in ICT security** is estimated by Gartner on an annual basis. Based on Gartner's regular forecasts from 2012 up to 2020 of the percentage of global ICT security spending out of ICT spending and total revenues, as well as taking account of the latest sector-specific Gartner data available to the Commission<sup>205</sup>, an assumption was made for the purposes of this impact assessment that the **average ICT security spending per sector in 2020 is of approx. 9.14% of the ICT spending**. Depending on the level of cybersecurity maturity and capabilities of the sector, as well as the level of digitalisation, an adjustment of +/-3% could be made to this average. Furthermore, the average ICT spending per sector is estimated to approximately 5.69% of the total turnover and hence **the average ICT security spending of the total turnover per sector in 2020 is estimated to approx. 0.52%**. For more details on the methodology aspects in relation to the average estimates above, see Annex 3.

The above-mentioned estimates used as a basis for this impact assessment are however conservative. A study on NIS investments commissioned by ENISA and implemented by Gartner (hereinafter called 'the NIS investments study')<sup>206</sup> indicates a lower level of ICT security spending in Europe, of about 6% of the ICT budget since 2016, with the banking, financial services and pharmaceuticals organizations having a ratio higher than 5%, while sectors like transport, education and retail would have the lowest such ratios, below 2.5%.

Indeed, some sectors or services have a more significant or faster growth of ICT security investment than others. For example, according to 2020 Gartner estimates and forecast, 8 of 10 cybersecurity markets are projected to grow faster than the market average, with cloud security growing the fastest.<sup>207</sup> In the banking sector, a survey by Deloitte and FS-ISAC<sup>208</sup> shows that, on average, banks, insurers, investment management firms and other financial services companies spend between 6% and 14% of their ICT budget on cybersecurity, with an average of 10%. Another survey by Deutsche Bank on cyber security spending by financial institutions<sup>209</sup> found that, on average, around 10% of financial institutions are below the 6%-14% range mentioned above.

For **options 2 and 3**, for the new sectors, subsectors and types of services, new compliance costs stemming from the NIS obligations would be borne. The NIS review

---

<sup>204</sup> Data still incomplete at the time of the writing of this Impact Assessment report.

<sup>205</sup> i.e. data available in the impact assessment supporting the NIS Directive.

<sup>206</sup> The first report of the study commissioned by ENISA on NIS investments was published on 11 December 2020: <https://www.enisa.europa.eu/publications/nis-investments/>.

<sup>207</sup> Cloud security is the smallest, fastest-growing cybersecurity market segment with a projected growth of 33% in 2020 up to approx. EUR 494: <https://www.forbes.com/sites/louiscolumbus/2020/08/09/cybersecurity-spending-to-reach-123b-in-2020/#766ad2a0705f>

<sup>208</sup> Referred to in the Impact Assessment for the Digital Resilience Act for financial services, SWD(2020) 203 final, p.43: <https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>

<sup>209</sup> [https://www.db.com/newsroom\\_news/Deutsche\\_Bank\\_Investor\\_Report.pdf](https://www.db.com/newsroom_news/Deutsche_Bank_Investor_Report.pdf)



country visits and the NIS review study surveys revealed that most of operators and service providers are following international standards when it comes to security requirements.<sup>210</sup> This made it difficult to separate the impacts of the NIS Directive on the ICT spending at the level of the organisations from the overall impact of the evolution of international security. The new security requirements considered under policy options 2 and 3 would be risk management based and would largely follow the existing international standards and practices of the majority of Member States. Furthermore, the incident notification obligations would be streamlined to provide more clarity on content, template and time of submission, thus keeping to a minimum the additional administrative burden on businesses.

The overall global ICT security spending<sup>211</sup> increased with approximately 22% from 2017 (the year after the entry into force of the NIS Directive) until 2020. While this increase is not directly linked to the NIS Directive, one can assume nevertheless that it also integrates the spending generated by security requirements such as those provided by NIS which largely follow international standards. Therefore, the assumption that in the medium-term (three to four years), the **new sectors** to be added to the NIS scope would entail **about 22% increase in their ICT security spending** would be a conservative assumption, most likely an overestimate, since it would consider a premise where the only trigger for extra ICT security investment would be the NIS framework. This would translate into ICT security spending in average per sector reaching about 11% of the ICT spending and 0.63% of the total turnover in three to four years from the entry into force of the revised NIS Directive. Yet, many other factors would naturally contribute to such increase, such as evolution of technologies and threat landscape, GDPR and other regulatory obligations, effects of particular incidents that may occur in the meantime or major crises, level of awareness, level of digitalisation, etc.

Based on 2018 Eurostat data, the following examples of **estimated average sector-specific costs for medium and large companies** translating the 0.63% increase in spending out of annual turnover in a time-span of 3-4 years for the **new sectors** considered for the NIS scope can be provided (*see also the detailed data on turnover and number of companies per sector in Annex 3*):

- Chemicals (manufacture): a total increase of EUR 2.70 billion per sector and EUR 0.85 million per company.
- Waste management: an increase of EUR 0.7 billion per sector and EUR 0.26 million per company.
- Wastewater: an increase of EUR 68 million per sector and EUR 0.14 million per company.
- Manufacture of:
  - ✓ food products: an increase of EUR 3.7 billion per sector and EUR 0.63 million per company.
  - ✓ beverages: an increase of EUR 0.55 billion per sector and EUR 0.53 million per company.
  - ✓ basic pharmaceutical products and pharmaceutical preparations: an increase of

---

<sup>210</sup> 37% of the respondents to the NIS study surveys targeting OES and 22% of the survey targeting DSPs considered that the adoption of the NIS Directive has affected their organisations as far as additional security requirements are concerned.

<sup>211</sup> <https://www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/>

EUR 1.32 billion per sector and EUR 1.41 million per company.

- ✓ computer, electronic and optical products: an increase of EUR 1.58 billion per sector and EUR 0.65 million per company.
- ✓ electrical equipment: an increase of EUR 1.9 billion per sector and EUR 0.55 million per company.
- ✓ machinery and equipment n.e.c.: an increase of EUR 3.95 billion per sector and EUR 0.44 million per company.
- ✓ motor vehicles, trailers and semi-trailers: an increase of EUR 6.85 billion per sector and EUR 2.33 million per company.
- ✓ other transport equipment: an increase of EUR 1.4 billion per sector and EUR 1.32 million per company.
- Postal and courier services: an increase of EUR 0.38 billion per sector and EUR 0.45 million per company.
- Food supply: an increase of EUR 3.27 billion per sector and EUR 0.62 million per company.

**For the sectors currently covered by the NIS Directive**, as compared to the new ones considered to be brought under the NIS scope in *options 2 and 3*, a rather limited increase of ICT security spending would be expected in the coming three to four years, just slightly over (+4-5%) the pace of ICT security spending increase forecasted by Gartner in December 2019, prior to the COVID-19 crisis: i.e. **about 12% increase in the ICT security spending**.<sup>212</sup> This would translate into ICT security spending in average per sector reaching about 10.2% of the ICT spending and 0.58% of the total turnover in three to four years. Measures such as the alignment of reporting obligations are expected to even diminish to a certain extent the administrative burden on the entities currently covered under the NIS scope.

Based on 2018 Eurostat data, the following examples of estimated **average sector-specific costs for medium and large companies** translating the **0.58% increase in spending out of annual turnover** in a time-span of 3-4 years for the **sectors currently covered by the NIS scope** can be provided (*see also the detailed data on turnover and number of companies per sector in Annex 3*):

- Electricity and gas: a total increase of EUR 6 billion per sector and EUR 1.94 million per company.
- Air transport: an increase of EUR 0.27 billion per sector and EUR 1.18 million per company.
- Drinking water supply and distribution: an increase of EUR 0.14 billion per sector and EUR 0.16 million per company.

In *option 2*, the extension of the NIS scope may lead to a potentially high administrative burden raised by the security requirements and reporting obligations for all companies concerned, and in particular for SMEs. Equally, given the wider scope of application, competent authorities would also have to invest additional considerable resources in the identification process and apply supervisory measures for a significantly higher number of companies, potentially requiring further refined strategies, including on prioritisation

---

<sup>212</sup> <https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem>.

policies and supervisory means and methods, as well as additional resources. For **option 3**, due to the differentiation in the level of obligations between the essential and important entities, for the latter, the compliance costs would be more reduced. Furthermore, in option 3, a size cap would be applied to exclude from the NIS scope micro and small enterprises. This would reduce furthermore the coverage of companies impacted by the NIS framework.

- ***Estimated costs<sup>213</sup> of the policy options at the level of organisations***

The identification of OESs and overview of DSPs, which have raised particular issues in practice, would remain unaddressed in **option 2**. As a result, the **administrative burden and compliance costs** would remain uneven for similar companies across Member States as they would be subject to different identification processes or not systematically considered digital service providers in all Member States where they conduct such activities. Businesses would therefore continue to bear a burden of uncertainty, with potential negative effects on the resources and prioritisation given to cybersecurity measures and compliance with the cybersecurity requirements and obligations, since the identification process is not being sufficiently clear. In particular, companies operating in such sectors in several Member States would continue to be subjected to different identification processes or none whatsoever.

In **option 3**, a general obligation would be introduced for the entities operating in the sectors and providing the services covered by NIS, while also excluding as a rule from the NIS scope all micro and small entities. This would by default exclude any administrative burden or unequal treatment imposed on companies across Member States triggered by divergences in the identification process or by legal uncertainty that could have affected the business planning or investments of these companies. Although option 3 would also allow exceptions, as explained in *section 6.1*, including the possibility for Member States to include in the NIS scope micro or small entities justified by their specific importance at regional or national level for that particular sector or other interdependent sectors or services, this would concern rather limited situations, decided on a case by case basis, and is unlikely to lead to notable administrative burden on competent authorities.

In option 3, digital service providers may have to register with ENISA, so that an EU-level overview of DSPs is available at Union level. This would however entail only very marginal one-off administrative costs that would not require additional staff or resources (i.e. more likely one-off 0.5 FTE<sup>214</sup> task).

The main costs incurred by companies stemming from the NIS framework are **compliance costs**, in particular related to the implementation of **security requirements** (i.e. risk management obligations), **reporting obligations** (i.e. incident reporting obligations) and application of **supervisory measures** (i.e. documenting compliance through audit reports, results of tests, scanning, etc.). In the survey targeting OESs and DSPs conducted by the NIS review study, both categories of respondents considered that the most significant compliance costs borne from the NIS obligations are those

---

<sup>213</sup> At the level of individual organisations, the cost of cybercrime is typically estimated as the cost of the activities by criminals gaining illicit access to victims' computers or networks. The elements of cybercrime cost would typically include: the loss of business confidential information; financial manipulation; opportunity costs, including disruption in production or services; buying cyber insurance, paying for recovery from cyberattacks; reputational damage and liability risk (*CSIS, McAfee (2018), Economic Impact of Cybercrime-No Slowing Down*).

<sup>214</sup> Full Time Equivalent.

concerning the *risk management measures*<sup>215</sup> and the *prevention and mitigation of impact of incidents*.<sup>216</sup> Fewer respondents<sup>217</sup> considered compliance costs raised by incident notifications (including cross-border) to be significant. Only 37% of the OESs respondents and 22% of the DSPs respondents considered that they have been affected by the additional security requirements introduced by the NIS Directive.

The NIS investments study indicates that, from the 251 organisations covered by the study in five Member States, 42.7% had a dedicated NIS Directive-related project or programme of between EUR 100,000 and EUR 250,000, with an average budget for NIS implementation projects of about EUR 175,000. A little under 50% of these organizations had to hire up to 4 FTEs. The majority of the affected organisations did not require additional staff to implement the NIS Directive. Data from the same study indicates that the three main areas of spending are: (i) vulnerability management and security analytics, with a share of 20%; (ii) governance, risks and compliance with a share of 18%, and network security with a share of 17%. The study found that the distribution between the different functional areas has been quite stable over the last four years, but it varies greatly between industries. As of 2020, information security staff<sup>218</sup> represents 5.6% of total ICT staff, measured in terms of FTEs.

In 2019, the majority of EU enterprises (65 %) reported that the ICT security related activities were carried out by external suppliers, while, responding to a different question, 40 % of the enterprises reported that the ICT security related activities were carried out by own employees.<sup>219</sup> **Options 2 and 3**, given the further harmonisation of risk management requirements, and even more in case of **option 3**, the introduction of new measures such as those targeting supplier relationship risk management or data storage-related risks, are expected to increase the sophistication of security measures implemented and hence the need for outsourcing or, alternatively, further specialisation of staff on cybersecurity aspects. This would however bring longer term benefits both for the cyber resilience of companies, the capacity to recover speedily following potential cyberattacks and mitigate damage. It may also bring benefits to the level of maturity and development of the European cybersecurity market due to a potential increase in demand of more specific technical services. Furthermore, the security requirements imposed in options 2 and 3 would be risk management based, therefore any investment in security measures would be proportionate to the cyber risks.

The IPACSO report stressed that the actors involved are rational or at least '*predictably irrational*'<sup>220</sup>, therefore they tend to maximize the payoff by minimizing the effort to achieve a goal, normally acting under conditions of scarce resources. This usually leads to underinvestment in cybersecurity measures. According to the report, an incentive structure to convince actors to adopt cybersecurity technology or a framework to improve adoption of cybersecurity would be one of the most effective ways that could lead to an increased cybersecurity investment. This is also the conclusion of the Ponemon Report, which points to automated security measures as one of the main cost saving factors in the context of potential data breaches. **Option 3**, as compared to option 2, would notably include measures that require a more thorough risk management approach, as well as

---

<sup>215</sup> 73% for OESs and 56% for DSPs.

<sup>216</sup> 73% for OESs and 56% for DSPs.

<sup>217</sup> 43-49% for OESs and 33-44% for DSPs.

<sup>218</sup> Information security personnel includes in-house and contract full-time equivalents supporting the IT security domains.

<sup>219</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT\\_security\\_in\\_enterprises#ICT\\_security\\_in\\_EU\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises#ICT_security_in_EU_enterprises)

<sup>220</sup> IPACSO Report, page 8, reference to Ariely, 2008.

policies such as coordinated vulnerability disclosure, allowing the use of additional channels of discovering vulnerabilities or the mutual assistance mechanism, which would lead to joint operational actions across borders. Such measures are expected to incentivise investment in cybersecurity technology and measures.

In relation to **reporting obligations**, as shown by the NIS review country visits, many OESs notify few significant incidents to competent authorities, some in the range of 1-2 per year. Typically DSPs would report no significant incidents in the vast majority of the Member States. The NIS investments study indicates that 81% of the organisations surveyed have established a mechanism to report incidents requiring no more than 4 FTEs for a large majority of respondents. The envisaged changes brought by options 2 and 3 would be expected to increase this reporting rate and further incentivise reporting beyond incidents to events such as near misses or vulnerabilities. However, while in appearance this would bring more cumbersome requirements as compared to the baseline scenario, since the incident notification obligations would be more prescriptive on the format, timeline and content, they would, at the same time, allow more legal certainty and clarity expected to translate in more efficient use of human resources. Furthermore, as shown by the NIS review study survey, incident notification is considered less costly by the organisations as compared to risk management requirements.

When it comes to **supervision and enforcement**, **option 2** would only introduce a set of principles for supervision and enforcement, while **option 3** would introduce a minimum level of requirements for competent authorities in relation to supervisory actions that they can apply (e.g. frequent or ad hoc audits, inspections, etc), as well as a minimum level of penalties. Since the likelihood of application of dissuasive penalties, including administrative fines, is expected to increase (notably with option 3), as opposed to the baseline scenario, businesses may instead increase ICT security investments and hence face higher compliance costs to avoid such penalties. More importantly, since the intensity of supervisory actions would most likely increase, businesses would bear additional compliance costs for documenting compliance. For example, according to DESI, less than half of enterprises reported maintaining log files for analysis after security incidents (45 %).<sup>221</sup> In **option 3** in particular, such costs would be alleviated for entities in sectors and providing services considered important, yet not essential, to which only an *ex post* supervisory regime would apply, and which therefore would not be required to systematically create and preserve evidence on compliance. In **option 2**, the compliance costs in this regard would instead increase for the DSPa who would pass from an *ex ante* supervisory regime to a fully-fledged one, which would entail *ex-ante* supervision and evidence-producing.

As regards **cooperation and information sharing**, **options 2 and 3** would further incentivise the setting up and participation in PPPs and ISACs with participation of public authorities. While the setting up and participation in these platforms can indeed be costly, it would only be on a voluntary basis and the benefits would outweigh such costs, since it would lead to a trusted network of secure exchange of valuable information which can help reduce cybersecurity costs in an organisation.<sup>222</sup>

---

<sup>221</sup> <https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020>

<sup>222</sup> See also ENISA's report of 2019 on Information Sharing and Analysis Centres (ISACS) – Cooperation Models: <https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models>

- *Estimated benefits of policy options at the level of organisations*

The 2015 Cost of Cyber Crime Study conducted by the Ponemon Institute<sup>223</sup> found that the **median annualized cost of cyber crime** was of approximately **EUR 4.63 million**. For the purposes of **weighing costs and benefits notably for options 2 and 3**, the NIS review study<sup>224</sup> **developed a modelling** starting from this annualized cyber crime cost, used as a proxy for the cost of a cybersecurity incident. This was referenced to an Eurostat estimate of about 450 cybersecurity incidents in 2019 involving critical infrastructures like health, finance and energy.<sup>225</sup> According to the modelling, the difference between options 2 and 3 is given by the difference of the cost of incidents compared to the baseline over a 10-years period, leading to the estimation that **option 3** is the most impactful with a **reduction in cost of cybersecurity incidents by EUR 11.3 billion**, as compared to EUR 8.3 billion in option 2. *See Annex 10.*

Furthermore, as mentioned above, the 2020 Annual Cost of a Data Breach Report of the Ponemon Institute, estimated the **average cost of a data breach**<sup>226</sup> to be **EUR 3.5 million in 2018**, an increase of 6.4 % over the previous year<sup>227</sup>, while at the level of various sectors the increase for the same reference period was even higher (10% to 13%). The same report found that the **average time to identify and contain a data breach is of 280 days**. At the same time, considerable differences were found among sectors: in healthcare, the lifecycle of a breach averaged 329 days, while the average lifecycle was 96 days shorter in the financial sector. Fully deployed security automation (e.g. use of advanced technology, AI, automated scanning tools) helped companies reduce the lifecycle of a breach by 74 days compared to companies with no security automation deployment, from 308 to 234 days. The report found that **lost business costs accounted for nearly 40% of the average total cost of a data breach, i.e. about 1.30 million EUR**. Lost business costs included increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation. The lowest cost was for notification of the data breach, 6% of total cost.

The NIS investments study indicates that 43% of the organisations surveyed in 2020 experienced cyber incidents with a direct financial impact of up to EUR 500,000.

Compared to the overall high level of costs, **an average increase of ICT security spending per sector for the next three to four years ranging from about 12%<sup>228</sup> to 22%<sup>229</sup>**) would lead to a **proportionate benefit of such investments** and even considerably exceed the costs for some sectors.

---

<sup>223</sup> [http://www.cnmeonline.com/myresources/hpe/docs/HPE\\_SIEM\\_Analyst\\_Report\\_-\\_2015\\_Cost\\_of\\_Cyber\\_Crime\\_Study\\_-\\_Global.pdf](http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf)

<sup>224</sup> interim findings of the NIS review study to be included in its final report due by December 2020/January 2021 [not yet submitted at the time of the writing of this report].

<sup>225</sup> <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>

<sup>226</sup> Data breaches can be considered a subset of cybersecurity incidents. This is because many security incidents mainly affect personal data. A data breach occurs when a cybercriminal infiltrates a data source and extracts confidential/private information. Most data breaches are attributed to the most common cybersecurity incidents, such as hacking or malware attacks, ransomware, denial of service, phishing.

<sup>227</sup> Annual Cost of a Data Breach Report, 2020, conducted by the Ponemon Institute, and based on quantitative analysis of 524 recent breaches across 17 geographies and 17 industries: <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>

<sup>228</sup> sectors already covered by the NIS framework.

<sup>229</sup> additional sectors and type of services to be covered by the NIS framework under options 2 and 3.

As regards the benefits stemming for specific measures, in **option 3, the replacing of the identification process with a generally applicable obligation** will reduce the administrative burden and unequal treatment of companies across Member States that led to legal uncertainty affecting business planning or investments.

**Options 2 and 3** would indeed provide more harmonised security requirements. This would entail, in particular, more clarity and alignment in defining the elements that the **security measures** at the levels of organisations should include (e.g. organisation of Information Security, human resources security, asset management, access control, encryption, physical and environmental security, supplier relationship assessments, etc). These measures would most likely incur compliance costs that, notably for less mature organisations, would require additional investments. According to Eurostat<sup>230</sup>, in 2019, 92% of EU enterprises with 10 or more persons employed used at least one measure in order to ensure integrity, authenticity, availability and confidentiality of data and ICT systems. One in three enterprises (33 %) reported having documents on measures, practices or procedures on ICT security. In one in four enterprises (24 %) these documents were defined or reviewed in the last 12 months. Enterprises less frequently used encryption techniques for data, documents or e-mails (38 %), ICT security tests (35 %), ICT risk assessment (33 %) and user identification and authentication via biometric methods (10 %).

Compliance costs that entail additional investments in automated security can only benefit companies in the medium and long term and reduce business loss. It is therefore expected that in **options 2 and 3** the short and medium term investments required by the reinforced **risk management requirements** would be less costly for companies which have deployed security automation. The Ponemon Report<sup>231</sup> concluded that businesses that had not deployed security automation saw an average total cost of EUR 5.15 million, more than double the average cost of a data breach of EUR 2.09 million for businesses that had fully deployed security automation. The report also showed the importance of incident response preparedness, as it was found to be the highest cost saver for businesses. The average total cost of a data breach for companies with an incident response team that also tested an incident response plan using exercises or simulations was EUR 2.81 million, compared to EUR 4.52 million for companies with neither such team nor tests of such plan. On a medium and long-term perspective, the investments in security automation and incident report preparedness would therefore lead to significant benefits for businesses. As shown by empirical evidence, while basic cybersecurity measures allow for better detection of incidents, more sophisticated measures, that indeed would require more investment, would help prevent incidents and on the long-term reduce costs for handling incidents and mitigating potential loss.<sup>232</sup>

In **option 3**, Member States would be encouraged to create a **single entry point for notifications concerning security breaches** stemming from the NIS Directive, the General Data Protection Regulation and the ePrivacy Directive would help further reduce the administrative burden and compliance costs on companies.

---

<sup>230</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT\\_security\\_in\\_enterprises#ICT\\_security\\_in\\_EU\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises)

<sup>231</sup> Annual Cost of a Data Breach Report, 2020, conducted by the Ponemon Institute: <https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf>

<sup>232</sup> *Cyber incidents, security measures and financial returns: Empirical evidence from Dutch firms*, Milena Dinkovay, Ramy El-Dardiry and Bastiaan Overvesty – CPB Netherlands Bureau for Economic Policy Analysis, 25 May 2020.

In the financial sector, the Commission's DORA proposal aims at bringing rules addressing ICT risk in finance together into a single legislative act which will be a *lex specialis* to the NIS framework. The requirements for financial entities would revolve around specific capabilities and functions in ICT risk management.<sup>233</sup> Financial entities would be required to put in place basic security measures.<sup>234</sup> These would not go beyond what will be required by the NIS framework under *options 2 and 3*, and therefore no additional compliance costs would be triggered in this regard. On the contrary, the Commission proposal envisages more specific requirements on aspects such as digital operational resilience testing<sup>235</sup> or monitoring of third-party risk through harmonisation of contractual aspects and a Union Oversight Framework. Moreover, the compliance costs and administrative burden on the operators of financial services is expected to be further reduced due to the introduction of one-stop-shop and the simplification of reporting obligations. Furthermore, the DORA proposal provides for the establishment of a management process to monitor, classify and report major ICT-related incidents to authorities responsible for the supervision of financial entities. These authorities will have to provide details of ICT related incidents to other institutions or authorities and in particular the NIS single contact points (SPOCSs). Financial entities will therefore benefit from harmonised ICT-related reporting content and templates. The proposal prepares the ground for a centralisation at EU level of ICT-related incident reporting. The European Supervisory Authorities (ESAs), the European Central Bank (ECB) and ENISA are mandated to assess and report on the feasibility of establishing a single EU Hub for major ICT-related incident reporting by financial entities.

The overview of the costs and benefits expected at the level of individual companies, notably for option 3 is presented in *Annex 3, section 2*.

### *SMEs*

In line with the vast majority, OPC respondents representing SMEs in the digital sectors deemed the cyber threat level to have increased significantly since 2016. They also share the view of other respondents that the level of preparedness of SMEs against cyber threats is relatively low in the Union (2 on a scale from 1 to 5). Asked about a potential expansion of the scope of the legal framework, they support the inclusion of certain sectors, such as manufacturing or data centres.

According to Eurostat, the ICT security measure “keeping the software or operating systems up-to-date” was used by almost all large (97 %) and medium sized (94 %) enterprises and more than 8 in 10 small enterprises (85 %). Similar figures were reported for the second most popular ICT security measure – the strong password authentication, which was used by 93 % of the large enterprises, 85 % of the medium size enterprises and 74 % of small enterprises. However, when it comes to more complex security measures, larger differences related to the enterprise size were observed, for example in the share of enterprises using the ICT risk assessment: 70 % of large enterprises, while the share of small enterprises using this particular measure was two and a half times smaller (28 %). This indicates that the administrative and compliance burden in relation to risk management measures is more evident in the case of SMEs.

---

<sup>233</sup> such as identification, protection and prevention, detection, response and recovery, learning and evolving and communication.

<sup>234</sup> e.g. set-up and maintain resilient ICT systems and tools that minimise ICT risk, business continuity policies and disaster and recovery, etc.

<sup>235</sup> i.e. periodical tests that would require development of specific tools.



According to DESI, in 2018, 13 % of enterprises in the EU experienced problems due to ICT related security incidents at least once.<sup>236</sup> This percentage was higher among large companies. ICT security incidents were reported by 23% of large enterprises, against 12% of SMEs. This difference might not necessarily indicate that SMEs are less likely to be affected by security incidents, but could also be the result of a lower reporting capacity of the latter. The most commonly reported problem caused by ICT security incidents was unavailability of ICT services, such as hardware or software failures, denial of service attacks, ransomware attacks, affecting 10 % of enterprises. Large enterprises were more likely to be affected by problems due to ICT related incidents; 25 % of large enterprises experienced such problems during 2018, while this was the case for 18 % of medium size and 12 % of small enterprises.

The pattern that ICT security related activities are relying predominantly on external suppliers was valid for both small and medium size enterprises. By contrast, the significant majority of large enterprises (83 %) reported the ICT security related activities being carried out by own employees.

The above-mentioned data shows that in the current NIS setting (*baseline*) and *option 2*, SMEs would bear more administrative and compliance costs than *options 3*, given that the latter would discard from the scope of the NIS framework small and micro businesses, which, as shown above, may represent a significant percentage of companies operating in a certain sector (for some even above 90%). As regards the level of ICT security spending, in option 3, medium enterprises could be expected to increase the level of spending in the three to four years following the introduction of the new NIS framework slightly more (e.g. +3%) than large enterprises, due to an increased need to outsource services in view of the new security and reporting requirements. Thus, for the new sectors or services, an increase of about 25% of ICT spending could be expected, while for the sectors and services already covered by the NIS Directive, an increase of ICT security spending of about 15%.

For the new sectors, this would translate into **ICT security spending in average per sector reaching about 11.4% of the ICT spending and 0.65% of the total turnover** in three to four years from the entry into force of the revised NIS Directive. Based on 2018 Eurostat data, the following examples of estimated average sector-specific costs for **medium companies** can be provided (*see also the detailed data on turnover and number of companies per sector in Annex 3*):

- Chemicals (manufacture): a total increase of EUR 0.7 billion per sector and EUR 0.28 million per company.
- Waste management: an increase of EUR 0.24 billion per sector and EUR 0.11 million per company.
- Wastewater: an increase of EUR 32 million per sector and EUR 0.078 million per company.
- Manufacture of:
  - ✓ basic pharmaceutical products and pharmaceutical preparations: an increase of EUR 96 million per sector and EUR 0.17 million per company.

---

<sup>236</sup> *Sample: In 2019, some 153 500 enterprises, with 10 or more persons employed, out of 1.48 million in EU-27 were surveyed. Out of these 1.48 million enterprises, approximately 83 % were enterprises with 10-49 persons employed, 14 % with 50-249 and 3 % with 250 or more.*  
[https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT\\_security\\_in\\_enterprises#ICT\\_security\\_in\\_EU\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises#ICT_security_in_EU_enterprises)

- ✓ computer, electronic and optical products: an increase of EUR 0.28 billion per sector and EUR 0.15 million per company
- ✓ motor vehicles, trailers and semi-trailers: an increase of EUR 0.3 billion per sector and EUR 0.15 million per company.
- Postal and courier services: an increase of EUR 21 million per sector and EUR 0.03 million per company.
- Food supply: an increase of EUR 1.4 billion per sector and EUR 0.3 million per company.

At the same time, in terms of benefits, raising the level of security requirements for these entities would also incentivise their cybersecurity capabilities and help improve their ICT risk management. This is even more relevant given that SMEs currently exhibit a relatively low level of cyber resilience.<sup>237</sup>

### **Public administration (from the perspective of the NIS scope) – policy options 2 and 3**

For the public sector, all Member States' institutions at central and regional levels have been considered for the NIS scope of the obligations, as they are all contributing to the smooth functioning of economy and society as a whole. In the same vein, as stressed by the EU Security Union strategy<sup>238</sup>, a framework of common rules on information security and on cybersecurity is being developed for all EU institutions, bodies and agencies, including mandatory and high common standards for the secure exchange of information and the security of digital infrastructures and systems.

In options 2 and 3, the NIS framework would only cover under 'public administration' central governments (i.e. all administrative departments of the state and other central agencies whose responsibilities cover the whole economic territory of a country), as well as the **major socio-economic regions (104** in total according to the *Nomenclature of territorial units for statistics*–NUTS 2021 classification) and the **basic regions for the application of regional policies (283** in total according to the NUTS 2021 classification).<sup>239</sup> No attempt was made for estimating the number of individual public institutions since the objective of the cost assessment is to make a global estimate of the total cost for the public sector.

Data for the public administration relate to the operating costs. ICT spending in the public sector is typically expressed as a percentage of the operating expenditure instead of revenues or turnover.<sup>240</sup> According to Eurostat<sup>241</sup>, in 2019, the total expenditure at **central government** level in the EU-27 was of 22% of GDP, while the total revenue was of 21.7% of the GDP. At the **local government** level, the total expenditure was the same as the total revenue: 10.9% of the GDP.

The NIS investments study indicates an average annual **ICT security spending** expenditure of 4% out of the ICT budget for governments in Europe. In line with the above-mentioned estimates of a 22% increase in the ICT security spending in the 3-4 years to follow the entry into force of the revised NIS Directive in option 3, the ICT

<sup>237</sup> The respondents to the OPC rate the level of preparedness of European SMEs with an average of 2.17 out of 5.

<sup>238</sup> COM(2020) 605 final, 24 July 2020.

<sup>239</sup> <https://ec.europa.eu/eurostat/web/regions/background>

<sup>240</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Total\\_general\\_government\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Total_general_government_expenditure)

<sup>241</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government\\_finance\\_statistics](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_finance_statistics)

security spending for governments would therefore be expected to increase to **4.88%** as a result of the intervention in this policy option.

Linked to the public administration category, under policy options 2 and 3, election authorities, technology and processes would also be covered under the NIS scope, as these are functional structures/frameworks for limited periods of time and are often under the responsibility of central, regional or local administrations.

### **Competent authorities**

The **administrative and compliance costs** currently borne by competent authorities (including CSIRTs, and SPOCs) are mainly stemming from the following NIS obligations: (i) development, monitoring and implementation of national strategies; (ii) identification process of OES, depending also on the system chosen at national level (self-assessment, registration, etc.); (iii) processing of incident reporting and interactions with companies linked to that; (iv) participation in the Cooperation Group and CSIRTs network; (v) cross-border operational cooperation or exchanges.

Due to the low level of harmonisation on the identification process, it appears, as also shown by the NIS review country visits, that in some Member States a significant amount of resources are dedicated to the *identification process*, notably when it involves self-assessment on the OES side or registration. In this context, the authorities need to conduct considerable work to identify, approach, guide and pursue companies to fulfil their obligations. The Member States' approaches to the OES identification process and the thresholds used (both quantitative and qualitative) vary considerably among Member States. Some operators are identified as OES via primary legislation, some via secondary legislation, some other through self-assessment and identification.<sup>242</sup> All these entail a certain administrative burden on the competent authorities that spend a considerable part of their resources on this process.

At the same time, there are **enforcement costs** borne by the competent authorities as a result of the supervisory obligations provided by the NIS Directive, notably in relation to OES. Since the supervisory activity for DSPs is lighter, being only *ex-post*, the costs incurred in terms of use of financial and human resources are much more reduced than in the case of OES. The lack of clarity on the DSP activities and the jurisdiction rule may however trigger the use of some resources that could have been spared should such rules and EU practices be more settled. As regards enforcement, as mentioned in *section 2.2.2.* above, it appears that Member States rarely pursue enforcement actions and apply almost no penalties. It would therefore be assumed that in the current setting this trend would continue and therefore few resources would be dedicated to such activities.

In **options 2 and 3**, additional **compliance and administrative costs** would be incurred by competent authorities.

As regards the *extension of the NIS scope* to additional sectors and services, including establishing an equal footing between OESs and DSPs, as well as a **reinforced approach on supervision**, overall the competent authorities are expected to supervise a notably higher number of entities, in particular in view of the additional sectors and types of services to be included under the NIS scope (*see above estimates per sector and type of service*). At the same time, in option 2 the OES identification process would be maintained, hence, at least for the current NIS sectors, it is expected for the number of entities supervised not to depart significantly from the current numbers. The new

---

<sup>242</sup> Over 50% of the OESs responding to the NIS survey were identified via other means than primary legislation.

provisions on security requirements would also trigger the need for a more pro-active approach and support to businesses, in particular in the newly added sectors. At the same time, the size cap to be applied in **option 3**, would filter through a considerable number of entities to be supervised by the competent authorities. Moreover, Member States' authorities would still need to establish prioritising strategies to supervise a wider range of entities. At the same time, for all entities considered 'important', only *ex-post* supervision would apply, thus triggering less administrative burden on the authorities.

From the NIS review country visits information, for some Member States which provided sufficiently granular data, it appears that typically about 15-20% of the staff of competent authorities (centralised or cumulated resources of decentralised authorities) conducts supervision-related tasks and about 30-50% handles incident-related work. Many Member States (13) have a heavily decentralised model, involving more resources and staff dedicated to specific sectors. The envisaged changes to the NIS scope, combined with the strengthening of the supervisory framework, including on DSPs, would lead to some increase in compliance costs for staff dedicated to supervisory activities. However, these costs would be balanced in **option 3** by the benefits of excluding small and micro entities and thus allowing the authorities to reallocate resources only for medium and large entities covered by a larger number of sectors.

**Option 2** would entail a heavier administrative burden and higher compliance costs for competent authorities as compared to **option 3**, also due to the fact that DSPs would be put on an equal footing with OES, with *ex post* supervision discarded, while at the same time the scope of sectors and services would be extended, with no size filter for entities and no differentiation of obligations imposed on businesses. Furthermore, the elimination of the OES identification process in **option 3** may also ease to some extent the administrative burden on some competent authorities, as the NIS review study targeted survey for OESs showed that about 27% of these were identified through actions of competent authorities.

Balancing all the above-mentioned factors, in **option 3** these new tasks are expected to require an overall **increase of about 20-30% of resources (including staff) of the relevant authorities per Member State at central level needed mainly for performing supervisory actions on a larger number of entities** (i.e. on-site and off-site checks, audits, requests for and assessment of compliance evidence, etc) **and interactions with industry (including sector-specific)**, while in option 2 of about 30-40%. The same additional compliance costs are estimated in relation to the cumulated resources of decentralised authorities per Member States<sup>243</sup>.

According to the in-depth interviews conducted by the NIS review study, competent authorities incurred NIS-related costs mainly linked to FTEs working on the NIS transposition and building the supporting organisation for OESs and DSPs, such as preparation or setting-up of national regulators in charge of the NIS Directive, upskilling human resources, expanding their capabilities to reach the right level of security maturity, and working and interacting with the whole ecosystem on this topic. **Option 3** is expected to lower the administrative burden triggered by unclear concepts or requirements which distracted competent authorities from core tasks. This is because option 3 would provide more clear-cut direct requirements for businesses and authorities, more legal certainty and predictability and less room for interpretation of concepts or thresholds. These changes are likely to lead in medium- and long-term to less cumbersome formalities and would allow authorities to better focus their resources on core cyber security tasks.

---

<sup>243</sup> a slight additional administrative burden may be triggered by the need to find sector-specific institutional solutions for the new sectors and services.

On *incident reporting*, currently the number of significant incidents reported by the competent authorities is rather low. For 2019, 15% of the Member States reported no significant incidents, while about 37% reported less than 10 significant incidents. Only three Member States reported 30 or more significant incidents and with more specific information on the type and impact of the incidents. This incident reporting rate is expected to increase in options 2 and 3. An assumption could be made that the vast majority of Member States would be able to report on average over 30 significant incidents per year. At the same time, in *option 3*, Member States<sup>244</sup> would also report the summary of the incident reports and relevant aggregated data to ENISA. Overall, the impact on the staff and resources necessary for handling incident notification and other similar reporting is expected to be rather limited, reflecting the expected increase in reporting from a wider range of sectors and services. In this regard, in both options 2 and 3 an **approximate increase of 10-15% in the staff of the competent authorities tasked to handle incident reporting** is estimated to be needed.

In *option 3*, the compliance costs for competent authorities would be incurred by the development of a number of specific cybersecurity-related policies, such as those regarding **supply chain security or coordinated vulnerability disclosure**. This may require some limited compliance costs at the level of policy staff, in the range of 2-3 FTEs per competent authority. The rest of the compliance costs on these aspects would be incremental to the additional resources required by the other new tasks mentioned above.

Furthermore, **additional enforcement costs** would be expected in *option 3* by the setting out minimum level of penalties. Considering that currently Member States have taken an approach towards enforcement that did not result in applying any notable penalties, this change in the NIS framework would trigger the need for additional resources and staff. As a rule, it would be expected for the staff conducting supervisory actions to also cover the aspects of enforcement of penalties. Nevertheless, in addition to the costs entailed by the supervisory tasks mentioned above, the strengthening of the enforcement regime would also lead to an increase of FTEs of legal experts, potentially 1-2 legal FTEs on average (new or reallocated) per competent authority would be expected.

In *option 3*, a peer review mechanism would be set up. This would entail regular on and off-site country-specific assessments conducted by cybersecurity experts designated by the Member States. The mechanism would therefore trigger certain administrative costs borne by competent authorities for the participation of designated cybersecurity experts in country visits and assessments. This may entail a number of an average of 4 country visits per year (costing about 5,000 EUR) for each competent authority.<sup>245</sup> These costs could however be partially supported through the Digital Europe Programme – Multiannual Financial Framework.<sup>246</sup>

*Option 3* would also entail setting up a crisis management framework which will build on CyCLONe. This is expected to trigger rather limited **administrative and compliance costs**. Member States would be required to designate competent authorities (either existing or new ones), set out regulatory plans and identify national capabilities, assets and procedures. However, these new requirements rather aim at connecting already existing institutions, frameworks and assignments so that to ensure the functionality of a cybersecurity operational angle for crisis management. Rather than requiring new departments or teams, the new framework is expected to build on existing ones. At

---

<sup>244</sup> Via SPOCs.

<sup>245</sup> e.g. travel and accommodation costs, daily allowances, expert days spent in one week country visits, preparation work, drafting work, etc.

<sup>246</sup> <https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme> .

institutional level, this may require a one-off start-up expenditure for new teams per Member State. This is likely to be covered by existing institutions (either in the ECI context or cybersecurity competent authorities) and would therefore require rather limited investment for the first two years, including 3-4 FTEs per Member State. The institutionalisation of EU-CyCLONE is likely to incur rather marginal costs, considering that the contact points at the level of the Member States are already designated and the main operational expenses incurred by the network would have already been included in national planning.

*Option 3* would also allow a shift in the mandate of the **Cooperation Group** that would reduce some of its administrative burden currently triggered by the lack of clarity and precision in the NIS Directive and would allow it to focus on more substantial/core tasks. For the CSIRTs, *option 3* would lead to some additional compliance costs, notably related to the increased role in implementation of policies such as the coordinated vulnerability disclosure, the implementation of the mutual assistance mechanism in cross-border cases, as well as the increase in the number of entities covered by the NIS scope. These costs would be reflected in additional FTEs (2-3), notably for the central CSIRTs teams per Member State, as well as potentially additional investment in technical equipment (software/hardware).

Overall, while option 3 appears to impose more administrative burden and compliance costs on the Member States authorities, on the medium and long term is also likely to bring substantial benefits to increased cooperation among Member States, including at operational level, as well as to incentivise an overall increase in and levelling of cybersecurity capabilities at national and regional level, through mutual assistance, peer-review mechanisms, better overview of and interaction with key businesses.

Mention should be made that the Member States would also be supported through the European Cybersecurity Competence Centre and its related network, as well as the funds made available through Digital Europe and Horizon Europe programmes.

The main costs and benefits relevant for national authorities for policy options 3 are summarised in *Annex 3, section 2*.

### **The EU Agency for Cybersecurity, ENISA**

The current NIS Directive, while not imposing specific obligations on ENISA, nor on operators or service providers as regards reporting to ENISA, resulted in additional work for ENISA in supporting the Member States in the implementation of the directive. ENISA is also acting as the secretariat of the CSIRTs network and is participating in the Cooperation Group. In *option 2*, no additional costs would be triggered for ENISA.

In *option 3*, the activities envisaged for ENISA are reinforcing existing tasks set within the limits of its existing mandate. While these activities would be covered by ENISA's general tasks according to its mandate, they will also result in additional workload for the agency. The main envisaged activities that would concern ENISA are those regarding: (i) the role of *observatory for state of cybersecurity in the Union (including conducting a regular survey)*; (ii) the *involvement in the peer-review mechanism*, where ENISA would support the Commission with the secretariat, as well as with participation of experts in peer-review missions (iii) the *registration of digital service providers with cross-border activities*, since in option 3 ENISA would be expected to hold a central registry of digital service providers operating cross-borders, which may require some dedicated software and/or database to be built up, (iv) the *depository and processing of aggregated data on notified incidents, as well as vulnerabilities newly discovered as a result of coordinated vulnerability disclosure policies*, which may require the upgrading or acquisition of additional software or database, (v) *ensuring the secretariat of CyCLONE*.

A considerable part of these envisaged activities would require a reshuffling of the existing resources of ENISA or reconsidering of certain priorities. It is also estimated that, in addition to the existing resources (including FTEs), ENISA would need 4-5 supplementary FTEs posts. At the same time, these envisaged tasks would provide additional benefits for ENISA, who would consolidate its role and standing in effectively supporting and developing EU cybersecurity policies. The competent authorities and the CSIRTs would also benefit from receiving tangible support from ENISA and better informing their cybersecurity decisions.

#### ✚ **Effects of the policy options on competitiveness and the level playing field in the Single Market**

**Option 2** is likely to have a positive, albeit relatively limited impact on ensuring a level playing field across Member States of all essential and important operators and DSPs, since all would be subjected to the same regulatory regime. For SMEs in particular, there are also likely negative impacts insofar as administrative burden is concerned, since they would be subject to the same obligations as larger entities, and also subject to same supervisory regime. **Option 3** is likely to have a positive direct impact on ensuring a level playing field across Member States of all essential and important operators and service providers. Furthermore, it is also likely to reduce cybersecurity information asymmetries among undertakings and incentivise the cybersecurity capabilities of SMEs.

A JRC report<sup>247</sup> stresses that currently users exert a rather minimal influence on vendors to provide solutions to revealed vulnerabilities, resulting in the delayed release of solutions or poor-quality solutions.<sup>248</sup> Stock prices of undertakings tend to be negatively affected by public knowledge of cybersecurity breaches only in the short term, while in the long term investors do not seem to substantially consider reputational damage. According to the JRC report, this would affect more the SMEs, making them vulnerable to cyber-attacks.<sup>249</sup> The report recommends incentivising cybersecurity information sharing to reduce information asymmetries. Option 3 focuses on improving operational cooperation and information sharing, through setting up frameworks to ensure that capabilities are brought together across the EU, mutual assistance mechanisms and joint supervisory action, incentivising information sharing, including on aspects such as coordinated vulnerability disclosure.

More clear-cut and harmonised security requirements for a conclusive pool of operators and service providers which are straightforwardly subjected to the NIS scope can also have positive effects on the development of the cybersecurity markets in Europe, increasing competitiveness thereof and investments in start-ups, new initiatives, etc.

## **7.2. Social impacts**

As presented throughout the report, cyber incidents can have far-reaching consequences for society. **Option 2**, by increasing the harmonisation of security requirements and expanding the NIS scope to a wider share of the EU economy, would be expected to contribute to some extent to achieving an improved level of cyber resilience across Europe. This may ultimately positively affect society, through a slightly improved protection level against the negative and/or disruptive effects of cybersecurity incidents.

---

<sup>247</sup> Cybersecurity – Our Digital Anchor, a European perspective, published in July 2020.

<sup>248</sup> ‘consumers often face high switching costs – i.e. they are not very likely to switch to a different provider in the case of known security weaknesses either concerning the software they use or in the software used by the vendors of the products and services they buy [...].’

<sup>249</sup> as ‘such vulnerabilities, which include a lack of formal cybersecurity policies, skills and expertise, shortage of financial resources, and incorrect attitudes towards risk management and cybersecurity, negatively influence their resilience to security threats.’

Such impact would however be rather limited, as in this option only targeted amendments would be brought to the NIS Directive, without changing the overall approach to ensure more sharing of responsibilities or a more hands-on approach to further align, upgrade and connect cybersecurity capabilities across Member States.

**Option 3** would generate a more extensive positive (indirect) impact on society than the other analysed options. The JRC Report recalls that: *‘Traditional measures to guarantee trust are no longer sufficient. [...] Cybersecurity should thus be considered as an essential societal need reinforcing the idea of a ‘digital society secure by design’. The rapid exploitation by cyber attackers on the COVID-19 pandemic to attack systems and individuals reinforces this need’*. Unlike option 2, option 3 would therefore go beyond such ‘traditional’ measures, in particular as regards operational cooperation and information sharing, as well as crisis management and supervision of cybersecurity compliance of private and public entities. This helps to ensure: (i) a higher level of cybersecurity for citizens; (ii) a high level of trust in business and cyber infrastructure and (iii) a high level of cyber resilience and ability to cope and prevent cyber incidents. Furthermore, with a more operational-oriented approach, this policy option could contribute to a greater extent to other social impacts, such as reduced levels of cybercrime and increased level of protection against cybersecurity incidents or data breaches. Increasing the level of cyber preparedness for businesses and other organisations may avoid potential financial losses as a result of cyberattacks, thus preventing the need to lay off employees.

### 7.3. Environmental impacts

No particularly significant environmental impact is expected for any of the policy options considered. However, increasing the overall level of cybersecurity could lead to the prevention of environmental risks/damage in case of an attack on a key service. This could be particularly valid for the energy, water supply and distribution or transport sectors. By strengthening the cybersecurity capabilities, the initiative could lead to more use being made of latest generation ICT infrastructures and services that are also environmentally more sustainable and to the replacement of inefficient and less secure legacy infrastructures. This is expected to contribute also to reducing the number of costly cyber incidents, freeing up resources available for sustainable investments. **Option 2** is expected to achieve such outcomes to a more limited extent, while **option 3** to a greater extent, as the latter is expected to lead to more robust cybersecurity capabilities.

### 7.4. Impacts on fundamental rights

Since maintaining the status quo (policy 0) would entail maintaining a certain level of cybersecurity, it may also have some limited impact on improving personal data protection, should it lead to some reduction in the number and severity of incidents including data breaches.

With **option 2**, increasing the level of cybersecurity and creating a level playing field for all operators falling in the scope of the NIS Directive by partially meeting the objectives mentioned above would most likely lead to improved personal data protection as a result of a reduced number and severity of incidents including data breaches. In **option 3**, the same type of impact would be as for policy option 2, with potentially more intensity given that this policy option is expected to lead to more robust cybersecurity capabilities and consequently would have a more substantial impact on the number and severity of incidents, including data breaches.

## 8. HOW DO THE OPTIONS COMPARE?

As regards the **effectiveness** of the policy options, **option 3** is most likely to meet the specific objectives to a high extent, while **option 2** would have potential to meet these



objectives in a more limited way. This is because **option 2** would introduce targeted changes to the current NIS Directive, with a view to clarifying certain provisions and improving harmonisation of the current rules. It would also cover additional (sub)sectors that are essential for the economies and societies of the Member States. However, this option would not change the overall approach and rationale of the legislative framework and would not allow a substantial change in relation to key processes, such as identification of OESs, operational cooperation and information sharing, crisis management or supervision and enforcement. These aspects, in relation to which problems were identified, as described in *Sections 1 and 2* above, would not improve in a meaningful way in the medium and long-term. The overall impact of this policy option on the specific objectives defined in *Section 5.2.* would therefore not depart significantly from the status quo. This would perpetuate shortcomings that lead to an insufficient and not comparable level of cyber resilience for key players in the Member States and shortfalls in relation to joint situational awareness. Instead, **option 3** goes beyond immediate fixes and entails a substantial change in approach towards the build-up of cybersecurity policies and measures across Member States. This would be notably done by consistent changes regarding key processes, such as the OES identification, bringing about shared responsibilities of various actors, public and private, and moving towards a more pragmatic and hands-on framework for operational cooperation, supervision and enforcement. The impact of this policy option on the level and effectiveness of cybersecurity across Member States is therefore likely to be high in the medium and long term, departing significantly from the status quo.

As regards the **economic impacts and efficiency**, of the three options, **options 2 and 3** would entail additional compliance costs due to the extension of sectoral scope. While the sectoral scope of the NIS framework would be considerably enlarged in both options, option 3 balances the burden that may be created by the NIS requirements, notably from the supervision perspective, on both the new entities to be covered and the competent authorities, by establishing a two layer approach, with a focus on big and key entities and a differentiation of supervisory regime that allows only *ex post* supervision (i.e. reactive and without a general obligation to systematically document compliance) for a large number thereof, notably those considered ‘important’ yet not ‘essential’.

For the **new sectors**, subsectors and services to be added to the NIS scope, an estimate of **about 22% increase in their ICT security spending** for the 3-4 years following the entry into force of the new framework was made as a conservative assumption. However, many other factors would naturally contribute to such increase, such as evolution of technologies and threat landscape, GDPR and other regulatory obligations, effects of particular incidents that may occur in the meantime or major crises, level of awareness, level of digitalisation, etc. For the sectors, subsectors and services already covered by the NIS scope, an estimate was made for an overall increase of about **12% of the ICT security spending** on a reference period of three to four years. Measures such as the streamlining of reporting obligations are expected to diminish the administrative burden on the entities currently covered under the NIS scope. Furthermore, the security requirements imposed in options 2 and 3 would be risk management based, therefore any investment in security measures would be proportionate to the cyber-related risks. For **option 3**, due to the differentiation in the level of obligations between the essential and important entities, for the latter, the compliance costs would be more reduced. Furthermore, in option 3, a size cap would be applied to exclude as a rule from the NIS scope micro and small enterprises.

As shown in *Section 7.1.*, the median annualized cost of cyber crime was estimated in 2015 to approximately EUR 4.63 million. Furthermore, the average cost of a single data breach was estimated to be EUR 3.5 million in 2018, with an annual increase of about

6.4% and about 10% to 13% at the level of various sectors. With this in mind, an average increase of ICT security spending per sector for three to four years ranging from 12% for the current NIS sectors up to a 22% for the new NIS sectors would lead to a proportionate benefit of such investments and even considerably exceed them for some sectors. At the level of individual companies, the compliance costs that may entail additional investments in automated security can only benefit companies in the medium and long term and reduce business loss.

Overall, while option 3 appears to impose more administrative burden and compliance costs on the Member States authorities, on the medium and long term is also likely to bring substantial benefits through increased cooperation among Member States, including at operational level, as well as to incentivise, through mutual assistance and peer-review mechanisms and better overview of and interaction with key businesses, an overall increase in cybersecurity capabilities at national and regional level.

As regards the benefits translated in reduction of costs of incidents, according to the modelling developed by the NIS review study, **option 3** would be most impactful with a **reduction in cost of cybersecurity incidents by EUR 11.3 billion over a 10-year period**, as compared to EUR 8.3 billion in **option 2**. *See also Annex 10.*

In relation to **social impacts**, **option 3** is more likely to generate a more extensive positive (indirect) impact on society than the other analysed options, mainly because it is more likely to increase the level and consistency of cyber resilience of key actors across the Union. Increasing the level of cyber preparedness for businesses and other organisations may avoid potential financial losses as a result of cyberattacks.

As far as **environmental impacts** are concerned, by strengthening the cybersecurity capabilities, options 2 and 3 may lead to more use being made of latest generation ICT infrastructures and services that are also environmentally more sustainable and to the replacement of inefficient and less secure legacy infrastructures. Option 3 would be expected to reach such achievements to a greater extent, since it would likely lead to more robust cybersecurity capabilities.

As regards **coherence with other legislation, initiatives or policy measures**, options 2 and 3 would further clarify the *lex specialis* rule (applicable, for example, in the case of financial services) and they would also bring providers of electronic communications networks or of publicly available electronic communications services under the NIS scope, thus allowing for more coherence of security requirements. Option 3 in particular, and notably its provisions on handling of supplier relationship security risks, would also ensure coherence with the upcoming cybersecurity certification schemes prepared by ENISA on the basis of the Cybersecurity Act, as well as with specific instruments such as the cybersecurity of 5G networks EU toolbox.

The extensive consultations held with all relevant categories of stakeholders, including the OPC and the consultations conducted in the context of the NIS review study (*see annexes 2 and 6*), have indicated that **both competent authorities and businesses** would largely support a revision of the current NIS legal framework, hence *options 2 and 3*. Both categories of stakeholders pointed to the need to address certain aspects or expressed support for certain new concepts or policy-related measures that would be promoted only via *option 3* (e.g. supply chain security policies, institutionalisation of an operational EU crisis management framework).

As regards the **proportionality of the intervention**, options 2 and 3 do not go beyond what is necessary to meet the specific objectives satisfactorily. The security measures and reporting obligations set out in both these options correspond to the Member States and businesses' requests to further clarify and harmonise the requirement level and would

help ensure a level playing field for similar entities across the EU, while at the same time levelling and raising the level of cyber resilience across Member States.

In option 3, the setting out of minimum requirements for supervisory action, enforcement and penalties is triggered by the need to ensure a better overview and level of compliance with the NIS framework at national levels. This would also be complemented by the mutual assistance mechanism and the joint supervisory actions in cross-border cases, the success of which would depend on the effectiveness and consistency of supervisory and enforcement measures applied across the Union. Furthermore, the current lack of practice at Member States level in the enforcement of dissuasive penalties comes counter to the NIS framework requirements on penalties. Given the general level of this principle, it is highly unlikely that systematic infringement actions could lead to any effective results. The supervisory and enforcement requirements envisaged by policy option 3 are nevertheless corresponding to practices already implemented in a number of Member States that appear to be considered by an increasing number of countries. Furthermore, the effectiveness of the increased harmonisation of security requirements and reporting obligations would equally depend on the effectiveness of supervision and enforcement. In the GDPR context, the enforcement system and prescriptive provisions on supervision and penalties have contributed to an increased level of compliance and, more importantly, to an increased level of security spending at corporate level. Some estimates indicate that regulatory compliance is being the most significant factor driving organizations' current spending on cybersecurity.<sup>250</sup>

As option 3 envisages setting a minimum maximum level of administrative fines, and as in many cases security incidents also entail a data breach, the new NIS legal act would provide that in such cases GDPR would have prevalence and administrative fines can only be applied once in that context. At the same time, this would not entail that more incidents would be notified to data protection authorities, rather it would be for the cybersecurity competent authorities to determine whether a data breach was concerned by the violation for which an administrative fine is being considered for NIS-related obligations.

---

<sup>250</sup> <https://www.sans.org/reading-room/whitepapers/bestprac/spends-trends-2020-cybersecurity-spending-survey-39385> and <https://www.zdnet.com/article/cybersecurity-this-is-how-firms-are-spending-their-budget-this-year/>

Impacts	Option 0: Baseline – Keep Status Quo	Option 2: Limited changes to the NIS Directive	Option 3: Systemic and structural changes and the adoption of a new legal act
Effectiveness	0	✓✓	✓✓✓
Economic/ Efficiency	0	✓	✓✓✓
Environmental	0	✓	✓
Social	0	✓	✓
Coherence (synergies with other relevant legislation)	0	✓✓	✓✓
Stakeholders' support	0	✓	✓
Proportionality	0	✗	✓✓
<b>Total</b>	<b>0</b>	✓✓✓✓✓✓✓✓ ✗	✓✓✓✓✓✓✓✓✓✓ ✓✓✓

**Table 5:** Overall impact of the various policy options. The symbols "✓" and "✗" indicate respectively positive (✓) and negative (✗) impacts as compared to the status quo. For each symbol a maximum a scale 1 to 3 (maximum positive or negative assessment) is used.

## 9. PREFERRED OPTION

### 9.1. Rationale and benefits of the preferred option

*Policy option 3 (systemic and structural changes to the NIS framework)* emerges as the preferred option based on the assessment of effectiveness against the specific objectives and efficiency of costs versus benefits. Policy option 3 focuses on clearly determining the scope of NIS application, extended to a more representative fraction of EU economies and societies, while streamlining requirements, along with a more defined framework for supervision and enforcement that would aim at increasing the level of compliance. It also entails measures aimed at improving policy building approaches at Member States level and changing the paradigm thereof, promoting new frameworks for supplier relationships risk management and coordinated vulnerability disclosure. At the same time, this policy option envisages mechanisms aimed at fostering more trust among Member States, both authorities and industry, incentivising information sharing and ensuring a more operational approach, such as the mutual assistance and the peer-review mechanisms. This option would also provide for an EU crisis management framework, building on recently launched EU operational network, and would ensure more involvement of ENISA, within its current mandate, in holding an accurate overview of the cybersecurity state of the Union.

In terms of efficiency, while the option would entail additional compliance and enforcement costs for businesses and Member States, it would also lead to efficient trade-offs and synergies, with the best potential out of all policy options analysed to ensure an increased and consistent level of cyber resilience of key entities across the Union that would eventually lead to cost savings for both businesses and society.

This policy option would lead to certain additional administrative burden and compliance costs for the Member States authorities. However, on balance, on the medium and long term would also bring substantial benefits through increased cooperation among Member States, including at operational level, as well as incentivising, through mutual assistance, peer-review mechanisms and better overview of and interaction with key businesses, an overall increase in cybersecurity capabilities at national and regional level. Policy option 3 would also ensure to a great extent coherence with other legislation, initiatives or policy measures, including sector-specific *lex specialis*.

As regards the choice of the legal instrument, i.e. directive, mention should be made that this would allow more leeway to the Member States in the preparations, compliance costs and expenses, hence easing the financial burden of an immediate compliance with new obligations. This may also bring benefits in terms of level of investments on the medium- and long-term, since a better spread of expenses over time would allow more thorough planning and gathering of supporting evidence and impacts analyses that allow more room for investment in research and innovative cybersecurity solutions and technologies. Furthermore, a number of envisaged provisions would be rather directed at Member States and would require further measures to be adopted at national level. From the consultations with the Member States, it appears that a significant number thereof are in favour of a directive rather than regulation.

### **9.3. REFIT (simplification and improved efficiency)**

According to the Commission's Regulatory Fitness and Performance Programme (REFIT), all initiatives changing existing EU legislation should aim to simplify and deliver stated policy objectives more efficiently (i.e. by reducing unnecessary regulatory costs and burdens).

The revised NIS Directive under the preferred option foresees a general exclusion of micro and small entities from the NIS scope and lighter *ex-post* supervisory regime applied to a large number of the new entities under the revised scope (so-called important entities – approximately 43,000 entities, *see also Annex 3 for more granular data*). These measures aim to minimise and balance the burden put on companies and public administrations. At the same time, the revised NIS Directive would extend significantly the sectors and number of entities covered and thereby increase the overall compliance burden for a big portion of the new companies, as well as the burden put on the public administrations in the context of supervision and enforcement. For that reason, the revised NIS Directive in the preferred option would contain concrete actions aiming at reducing the regulatory burden, as follows:

- Replacing the complex identification system for OESs with a generally applicable obligation (i.e. the size-cap rule) which is expected to reduce administrative burden on the authorities, create legal certainty and level the playing field for companies across the Union.
- A higher level of harmonisation of security and reporting obligations, which would decrease compliance burden, especially for entities providing cross-border services.
- The establishment of a central registry operated by ENISA for all providers of digital services which would help national administrations to clarify fast and without

spending excessive resources in investigations, where the main establishment of concrete entity is and identify the Member State with jurisdiction over that entity.

- The mutual assistance between Member States authorities and the possibility of carrying out joint supervisory measures foreseen would not only contribute to more effective enforcement, but also streamline administrative resources and ultimately alleviate administrative burden through synergies.
- The inclusion of electronic communications networks or services providers<sup>251</sup> and trust service providers<sup>252</sup> in the scope of the revised NIS Directive and the repeal of their respective security obligations from the eIDAS Regulation and the European Electronic Communication Code.
- Encouraging Member States to consider a single entry point for notifications concerning security breaches stemming from the NIS Directive, the General Data Protection Regulation and the ePrivacy Directive, as explained in the description of policy option 3.

---

<sup>251</sup> These are subject to security and incident notification obligations laid down in Article 40 of the European Electronic Communication Code. At the same time, these providers are subject to almost identical type of obligations under the NIS Directive as far as they also provide services included in the NIS scope such as IXP (Internet Exchange Points), DNS (Domain Name Servers) or cloud computing services.

<sup>252</sup> These are subject to security and reporting obligations under Article 19 of the eIDAS Regulation, which are similar to those laid down in the NIS Directive. However, digital certificates provided by those providers are frequently used as authentication factors in the provision of financial services, cloud computing services or other essential services that fall under the current NIS Directive. Therefore, any security incident affecting the trust services used as authentication means within the essential services might also affect the continuity of the essential service itself and thereby trigger a double reporting.

<i>REFIT Cost Savings – Preferred Option</i>		
<i>Description</i>	<i>Amount</i>	<i>Comments</i>
More harmonisation of security requirements, reporting obligations and supervisory and enforcement actions and more clarity on the scope by sectors and entities	The quantification of the actual effects of the harmonisation measures would not be possible due to the wide cross-sectors and cross-country differences, as well as the considerable differences in the level of cybersecurity maturity and investment for both businesses and national authorities. However, it is expected for the harmonisation measures to provide more certainty and a more effective cooperation among Member States, consequently easing the burden on both businesses and administrations which is currently generated by insufficient clarity or inconsistency of certain requirements (e.g. identification of OESs or thresholds for incident notifications) or jurisdiction rules (notably as regards DSPs)	Concerns businesses and national authorities

*Table 6: REFIT Cost Savings – Preferred Option*

#### **10. HOW WILL ACTUAL IMPACT BE MONITORED AND EVALUATED?**

A revised NIS Directive will have to strike the balance between placing additional burden on competent authorities and businesses on the one hand, and achieving a higher level of cyber resilience on the other hand. Eliminating cyberattacks and incidents entirely is not a realistic perspective and investment in cybersecurity, while essential, cannot go up to a level which would have a detrimental effect on the core business and financial viability of the company. This needs to be taken into account when defining how success can be measured.

A detailed table with monitoring indicators, expected targets and frequency of monitoring per indicator can be found in *Annex 11* for the general objectives and in *Annex 12* for specific and corresponding operational objectives. The assessment of indicators will be conducted by the Commission, with the support of ENISA and the Cooperation Group, starting 54 months following the entry into force of the new NIS legal act. Some of the monitoring indicators based on which the success of the NIS review would be assessed are as follows:

- **Improved handling of incidents:** By taking cybersecurity measures, companies are not only improving their ability to avoid certain incidents entirely, but also their incident response capacity. Measures of success are therefore i) the reduction of average time it takes to detect an incident, ii) the time it takes organisations on average to recover from an incident and iii) the average cost of a damage caused by an incident.
- **Increased awareness of cybersecurity risks by the top management of companies:** By requiring companies to take measures, a revised NIS Directive

would contribute to raising awareness of cybersecurity related risks amongst the top management. This can be measured by studying to which extent companies under the NIS scope are prioritising cybersecurity in internal company policies and processes as evidenced by internal documentation, relevant training programmes and awareness activities for the employees and prioritising security-related ICT investment. The management of all essential and important entities should also be aware of the rules laid down by the NIS Directive.

- **Levelling sector-specific spending:** ICT security spending varies considerably between sectors in the EU. By requiring companies in more sectors to take measures, deviations from the average sector-specific ICT security spending as a percentage of overall ICT spending should diminish between sectors and across Member States.
- **Stronger competent authorities and increased cooperation:** A revised NIS Directive would confer additional tasks on competent authorities. This would have a measurable impact on the financial and human resources dedicated to cybersecurity agencies at national level and should also have a positive impact on the capacity of competent authorities to proactively cooperate and therefore increase the number of cases where competent authorities are engaging with each other for the purpose of dealing with cross-border incidents or carrying out joint supervisory activities.
- **Increased information sharing:** The revised NIS would also improve information sharing among companies and with competent authorities. One of the targets of the review could be to increase the number of entities participating in the various forms of information sharing.

As highlighted throughout the impact assessment, while at global level there is a wealth of metrics in cybersecurity research and literature for measuring cyber threats and cybersecurity measures, there are still considerable gaps in the availability of systematic data to populate these metrics and in particular when it comes to measuring the effect of particular policy actions or returns of security investments. On top of this, such systematic indicators and data are missing for the EU level in particular.

For the reasons mentioned above, the preferred policy option analysed in this impact assessment also comprises a measure which aims at reinforcing an observatory role for ENISA, with the support of the Commission. This would enable, among others, the gathering of regular statistics and data on threats, incidents, resolves, capabilities and resources available, costs incurred, cross-border operational cooperation, research and innovation. A regular **report on the state of cybersecurity in the Union** will be published by ENISA. The findings of this report will also be used as a monitoring tool for the impact of the measures implemented through the preferred option.

At the same time, ENISA, supported by the Commission, will also develop a regular business survey, to be launched in 2021-2022, that would systematically monitor the impact of the NIS framework and assess regularly (i.e. on an annual basis) the level of cyber resilience of businesses across Europe. The survey would cover entities falling within the NIS scope and assess aspects such as awareness of cybersecurity policies<sup>253</sup> and implementation of cybersecurity policies within the organisation, measured through indicators concerning the strength and sophistication of security measures, control and

---

<sup>253</sup> e.g. the importance that the management of the organisation is giving to cybersecurity, how well are people being informed and trained, how is cybersecurity presented as a priority, etc.



capability to identify and manage risks<sup>254</sup>, resources available and fluctuations thereof, interaction with public authorities, occurrence, handling and impact of incidents.

---

<sup>254</sup> For example: use of tools for vulnerability management and disclosure, frequency and depth of vulnerability scans, use of information systems audit coordination, use of tools to handle supplier risks.



Brussels, 16.12.2020  
SWD(2020) 345 final

PART 2/3

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT REPORT**

*Accompanying the document*

**Proposal for a Directive of the European Parliament and of the Council  
on measures for a high common level of cybersecurity across the Union, repealing  
Directive (EU) 2016/1148**

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 344 final}

## Table of Contents

Annex 1: Procedural information .....	5
1.    Lead DG, Decide Planning/CWP references.....	5
2.    Organisation and timing .....	5
3.    Consultation of the RSB.....	5
4.    Evidence, sources and quality .....	5
Annex 2: Stakeholder consultation.....	7
1.    Introduction .....	7
2.    Consultation scope and objectives.....	7
3.    Consultation activities .....	7
4.    Results of the Open Public Consultation.....	10
Annex 3: Who is affected and how?.....	19
1.    Practical implications of the initiative.....	19
2.    Summary of costs and benefits.....	60
Annex 4: Methodology and criteria for determining the additional sectors, subsectors and services considered for the NIS scope in policy options 2 and 3 .....	70
Annex 5: Evaluation report .....	81

## Glossary

<i>Term or acronym</i>	<i>Meaning</i>
AI	Artificial Intelligence
CDN	Content delivery network
CSIRTs	Computer Security Incident Response Teams
CyCLONe	European Cyber Crises Liaison Organisation Network
DDoS	Distributed Denial of Service
DEP	Digital Europe Programme
DESI	Digital Economy and Society Index
DNS	Domain Name System
DORA	Digital Operational Resilience Act for the financial sector
DSP	Digital service provider
EASA	The European Union Aviation Safety Agency
ECCSA	European Centre for Cybersecurity in Aviation
ECI Directive	Directive on the identification and designation of European critical infrastructures
ECJ	European Court of Justice
EECC	European Electronic Communications Code
EMSA	European Marine Safety Agency
eIDAS (Regulation)	Regulation on electronic identification and trust services for electronic transactions in the internal market
ENISA	The European Union Agency for Cybersecurity

GDPR	General Data Protection Regulation
IaaS	Infrastructure as a service ( <i>cloud service model</i> )
ICS	Industrial control system
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union: The United Nations specialised agency for information and communication technologies
IXPs	Internet Exchange Points
JRC	European Commission's Joint Research Centre
LOTL	European List of eIDAS Trusted Lists
OES	Operator of essential services
OPC	Open public consultation
MeliCERTes	Cybersecurity Digital Service Infrastructure Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs
NACE	Statistical Classification of Economic Activities in the European Community
NIS Directive	Directive concerning measures for a high common level of security of network and information systems across the Union
NIST	National Institute of Standards and Technology – US Department of Commerce

PaaS	Platform as a Service ( <i>cloud service model</i> )
PPP	Private Public Partnership
ROSI	Return of Security Investment
SaaS	Software as a Service ( <i>cloud service model</i> )
SME	Small and medium-sized enterprises
SPOC	Single Point of Contact
TFEU	Treaty on the Functioning of the European Union
TLD	Top-level domain

## ANNEXES

### ANNEX 1: PROCEDURAL INFORMATION

#### 1. Lead DG, Decide Planning/CWP references

The lead DG is the Directorate-General for Communications Networks, Content and Technology. The Decide reference of this initiative is PLAN/2020/7447.

The Commission Work Programme for 2020 provides, under the heading *A Europe Fit for the Digital Age*, the policy objective of *Increasing cybersecurity*, the initiative for the *Review of the Directive on security of network and information systems (NIS Directive)* (legislative, incl. impact assessment, Article 114 TFEU, planned for Q4 2020).

#### 2. Organisation and timing

The Inter-service Steering Group was set up by the Secretariat-General to assist in the preparation of the initiative. The representatives of the following Directorates General participated in the ISSG work: Legal Service, HOME, JRC, TAXUD, DIGIT, GROW, FISMA, SANTE, MARE, DEFIS, MOVE, ENER, ECHO, EEAS, NEAR, AGRI, BUDG, REFORM, ENV, TRADE, ESTAT, HR, JUST, CLIMA.

The last meeting of the Inter-Service Steering Group took place on 15 October 2020.

An Inception Impact Assessment was published on 25 June 2020 and was open to feedback from all stakeholders for a period of 7 weeks.

The draft Impact Assessment report and all supporting documents were submitted to the Regulatory Scrutiny Board (RSB) on 23 October 2020, in view of a hearing on 18 November 2020.

#### 3. Consultation of the RSB

On 23 October 2020, the Directorate-General for Communications Networks, Content and Technology submitted the draft Impact Assessment to the Regulatory Scrutiny Board, in view of a hearing that took place on 18 November 2020.

#### 4. Evidence, sources and quality

The Commission carried out extensive preparatory work during the previous Commission's mandate. Conformity checks were undertaken with a view to assessing the compatibility of the national implementing measures with the NIS Directive's provisions.

Since June 2019, the Commission has also been organising country visits to gather feedback on the implementation and functioning of the Directive from numerous stakeholders. The Commission has collected information from a large number of stakeholders, including essential services operators, digital service providers and the national competent authorities. Moreover, under Article 23 (1) of the NIS Directive, based on the information provided by the Member States, the Commission adopted in October 2019 a report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services (hereinafter called the 'OES Report'). The Commission has collected feedback on the functioning of the NIS Directive from all participating Member States' authorities and the European Union Agency for Cybersecurity (ENISA) also in the framework of the NIS Cooperation Group.

The results from the country visits, the conclusions from the OES Report and feedback from the NIS Cooperation Group discussions fed into the evaluation of the functioning of the current NIS Directive according to Article 23(2) as well as into the impact assessment. In addition to above actions, the Commission also collected evidence via an open public consultation, desk research, expert interviews, workshops with experts and focus groups with representatives of national authorities of Member States and businesses in the relevant sectors under scrutiny, as well as other stakeholders.

As regards the economic impact, the impact assessment used available research on cybersecurity costs and cybercrime, as well as statistics mainly from sources such as: Eurostat and the Digital Economy and Society Index (DESI). However, as pointed out in the impact assessment, there are currently no available data comparable across the EU to measure the return of cyber security investment across sectors or per sector. While there are some models for the calculation of the returns of investment and in particular security metrics or cyber threat metrics, there is an overall absence of consistent data based on real cases that could support such metrics.

The NIS review process was also supported by a support study<sup>1</sup>, which was launched in April 2020 and has its final report due by the end of 2020. The study was implemented by a consortium made of Wavestone, CEPS and ICF and supported the review by: (i) conducting an evaluation of the NIS Directive, (ii) conducting an analysis of a wide range of policy measures to be considered for the options developed in the Impact Assessment, (iii) conducting targeted consultations consisting of surveys, interviews and workshops, (iv) processing the results of the open public consultation.

---

<sup>1</sup> Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665.



## ANNEX 2: STAKEHOLDER CONSULTATION

### 1. Introduction

A periodical review of the overall functioning of the [Directive \(EU\) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union](#) (“NIS Directive” or “the Directive”) is a legal obligation foreseen by Article 23 (2) of the Directive, according to which the Commission shall report to the European Parliament and to the Council for the first time by 9 May 2021. The review together with the impact assessment and a potential legislative proposal have been announced in the Commission Work Programme 2020 for Q4 2020.

Now, more than three years after the transposition deadline of the NIS Directive, all Member States have communicated to the Commission full transposition of the Directive into their national legislation.

In order to gather valuable feedback from all stakeholders interested in the review of the NIS Directive, the Commission organized several consultation activities addressed to different interest groups.

### 2. Consultation scope and objectives

The consultation activities aim at collecting the views of Member States competent authorities, Union bodies dealing with cybersecurity, operators of essential services (OES), digital services providers (DSPs), as well as economic entities that could potentially become OES and DSPs in light of NIS2, trade associations, researchers and academia, cybersecurity industry professionals, consumer organisations and citizens. All these different stakeholder groups have important information and insights on actions taken for the implementation of the NIS Directive, as well as interest in and opinions on shaping the debate about the possible options for the future.

The stakeholder consultation has two objectives:

- (1) To collect views on the implementation of the NIS Directive (to support the analysis on the retrospective evaluation of the Directive) ;
- (2) to collect views on the impacts of possible future changes to the legal act (to support the forward-looking assessment).

The Commission has issued the terms of reference for a study to assist in evaluating the existing legal and policy framework, identifying policy objectives and proposing and assessing expected impact of a limited number of policy interventions. The study is set to run for 10 months from April 2020 until January 2021.

### 3. Consultation activities

The consultation activities seek to obtain input on the five main evaluation criteria based on the [EU Better Regulation Guidelines](#) (effectiveness, efficiency, relevance, coherence, EU-added value) as well as the potential impacts of possible options for the future. Both the open public consultation and the targeted surveys developed by the contractor were structured according to the logic of the five criteria.

The following consultation activities were organised:

- ✓ **Targeted interviews** conducted by the Commission and in the framework of the report based on Article 23(1) of the NIS Directive, assessing the consistency of the approaches taken by Member States in the identification of operators of essential services required to implement cybersecurity measures (*OES report*). The Report was

published by the Commission on 28 October 2019 and was the first step towards the review of the NIS Directive. The Commission interviewed representatives from the competent authorities from nine Member States: Germany, Estonia, Croatia, Hungary, Lithuania, Malta, Poland, Portugal and Sweden.

- ✓ **The combined evaluation roadmap/Inception Impact Assessment.** It aimed to inform citizens and stakeholders about the Commission's work in order to allow them to provide feedback on the intended initiative and to participate effectively in future consultation activities. Citizens and stakeholders were, in particular, invited to provide views on the Commission's understanding of the current situation, problem and possible solutions and to make available any relevant information that they may have, including on possible impacts of the different options. The feedback period lasted from 25 June 2020 to 13 August 2020.
- ✓ **An Open Public Consultation (OPC)** with *questions targeting citizens, stakeholders and cybersecurity experts*. It included questions regarding all elements of the NIS Directive in order to gather information for the retrospective evaluation. It was also focused on policy options for a potential revision of the Directive. The aim was to collect diverse opinions and experiences from all stakeholder groups. A smaller set of questions was open to all participants. Respondents such as professionals in the field, or organisations with specific knowledge and expertise were directed to respond to a set of targeted questions within the same online survey. The Public Consultation, implemented according to the Commission's Better Regulation Guidelines for stakeholder consultations, was carried out for a 12-week period, starting on 7 July 2020 and closing on 2 October 2020. The questionnaire was made available in all 24 official EU languages, ensuring that the public consultation is accessible to as many stakeholders as possible, especially citizens. *206 replies* were collected online, of which *182* were replies provided by actors located in EU27. The Commission has received replies from a variety of different stakeholder groups, such as companies/business organisations, business associations, academic/research institutions, consumer organisations, EU citizens, non-governmental organisations (NGO), public authorities and trade unions.
- ✓ **Surveys** undertaken by the contractor, ENISA and the Commission targeting competent authorities, OES, DSPs and organisations that could potentially be included in the scope of the NIS Directive following its revision. While the contractor and ENISA carried out the surveys, the selection of questions and the identification of the target groups were carried out in close cooperation with the Commission. The survey questions supported both the retrospective evaluation and the identification of policy options for a potential impact assessment. Targeted online questionnaires were sent out in July 2020 with a deadline for replies set on 7 August 2020.

Three questionnaires were available online for all stakeholder groups: competent authorities with 46 respondents; OES with 49 respondents and DSPs with nine respondents. With regard to national authorities, 66% were centralised authorities, whereas remaining 34% were sectoral authorities. If it comes to centralised authorities, there was an equal participation of CSIRTs and Single Points of Contact (SPOC) – 37%, bodies representing both CSIRTs and SPOC contributed in 13% of replies and remaining 13% of respondents did not specify their functions. Most replies of national competent authorities were provided by Danish authorities (17%), followed by 13% replies provided by the Italian authorities, 9% replies from the Polish authorities, 7% responses of Finnish, the same percentage of questionnaire submitted by Dutch authorities and 4% of replies provided by authorities from

Bulgaria, Latvia, Luxembourg, Slovakia and Sweden. The rest of Member States provided replies that equal 2% of the total number of replies each.

Concerning the online survey aimed for OES, 67% of respondents represented OES currently covered within the NIS Directive, 14% described themselves as providers of essential services outside of the current scope of the NIS Directive and the remaining 18% ticked box 'Other' (ex. Financial sector collaborative defence and information sharing consortium, ATM/ANS, DSP, Cybersecurity researcher, EU Agency, Trade Association; Telecoms, Professional association; German Technical and Scientific Association for Gas and Water).

44% of respondents of the online survey addressed to DSPs are DSPs currently covered within the NIS Directive and 56% described themselves as 'Other' (ex. Providers of secure hardware for OES and DSPs, Information security company, Interested party, Cybersecurity company, Provider of security technologies)

- ✓ **In-depth interviews** carried out by the contractor. These interviews were conducted in order to gain a deeper understanding of current cybersecurity challenges, the evolving threat landscape and to discuss policy options for a potential revision of the NIS Directive. The experts were selected by the contractor upon consultation with the Commission. 16 interviews were conducted in the second and third quarter of 2020: four interviews with the competent authorities, seven with OESs, two with DSPs, two with the EU Institutions and Agencies and one with a Think-Tank.
- ✓ **Workshops organized by the contractor.** The workshops foreseen over the course of the study (Opening Workshop: June 2020; Intermediate Workshop: July 2020; Closing Workshops: 12 October 2020 for national competent authorities and 13 October 2020 for the private sector) are crucial to present and discuss the findings of the study, as well as to gather feedback from different groups of stakeholders active in the field of cybersecurity. Due to the COVID-19 crisis, all the workshops were held online.
  - *An Opening Workshop* took place as two separate virtual sessions on 8 and 11 June 2020 with 119 registered participants. It included an introduction to the NIS Directive review process by the unit on Cybersecurity & Digital Privacy Policy (DG CNECT), followed by an overview of the current approach to the review of the NIS Directive and the forward-looking impact assessment provided by the Project Team (presentation of the study, methodological approach, work plan and stakeholder engagement plan).
  - *An Intermediate Workshop* took place on 16 July 2020 with 144 registered participants. It provided participants with an update on the progress of the study to support the review of the NIS Directive including an overview of the different consultation activities. The preliminary findings coming from the evaluation of the functioning of the Directive were presented followed by a discussion with the participants on the impact of changes introduced by the NIS Directive since 2016 while assessing four main evaluation criteria: relevance, coherence, EU added-value, and effectiveness. This was followed by a session focusing on the high-level findings for the future policy measures and a discussion on those measures that are currently open to discussion throughout the review process, including the consultations with stakeholders.
  - *Two Closing Workshops* took place on 12 October 2020 (for competent authorities, gathering over 65 participants), and 13 October (for the private sector, gathering over 60 participants). The workshops aimed to engage the participating stakeholders in a reflection on potential policy options to further

enhance the level of protection of network and information systems across Europe and their respective economic, environmental and social impacts accounting for current and future technological developments. The evidence collected from the Closing Workshop was thus used to feed into the forward-looking element of the evaluation study; ensuring that subsequent EU policy action relation network and information systems is relevant, applicable and future proof.

- ✓ **Country visits** to gather information about the implementation of the NIS Directive and its functioning across the European Union. The Commission has started to visit Member States in spring 2019. It has completed this exercise in July 2020, after visiting all 27 Member States. Twelve of these visits took place virtually, due to travel restrictions linked to the COVID-19 crisis. During the country visits, the Commission interviewed *117 national competent authorities, 136 operators of essential services and 18 digital service providers*. Interlocutors were required to fill out a questionnaire covering all aspects of the implementation (such as national rules on OES identification, security requirements, incident notification and the cooperation with competent authorities). The Commission received and analysed *231 such questionnaires*.
- ✓ **Meetings of the NIS Cooperation Group and its work streams.** The Commission has gathered a wide variety of information about the functioning of the NIS Directive and its implementation by Member States since the Cooperation Group has been created in 2017. The Group gathers representatives from the competent authorities of all Member States and meets roughly four times per year. In addition, several *sectoral and topical work streams* have been created to discuss in-depth questions concerning the implementation of the NIS Directive in the Member States. The Commission is in constant dialogue with the national authorities in charge of the transposition and implementation of the NIS Directive. So far, two plenary meetings of the NIS Cooperation Group were focused on the review of the NIS Directive: the 15<sup>th</sup> meeting, which took place in June 2020 and the 16<sup>th</sup> meeting from September 2020. A *special meeting* of the Cooperation Group took place at the end October 2020.

#### 4. Results of the Open Public Consultation

##### ✓ **Profile of respondents**

*By country:* Respondents from Belgium were most numerous with 47 responses (22.8%), followed by 24 responses from Germany (11.7%), 18 responses from Austria (8.7%) and 17 responses from France (8.3%). Regarding countries outside the EU, 12 responses were received from the USA (5.8%).

*By participant type:* Trade associations representing both sectors covered by the NIS Directive and sectors that do not fall within the scope of the NIS Directive make up a third of the sample (68 responses) closely followed by companies covered by the NIS Directive, i.e. operators of essential services and digital service providers (57 responses). Other stakeholders (36 responses) include economic operators not covered by the NIS Directive, consumer organisations and EU bodies. 14 responses received were submitted by national competent authorities (CSIRTs included), while 10 responses were received from individual citizens.

##### ✓ **Relevance of the NIS Directive**

Respondents were asked to indicate the extent to which the **objectives of the NIS Directive are still relevant**. An overwhelming majority of the respondents indicated that the objectives of the Directive are still relevant, and even very relevant. To the

respondents, the most relevant objective of the three is to promote a culture of security across all sectors vital for the EU economy and society (77.2%). Similar response patterns were observed across different respondent categories.

#### ✓ **Cyber threat landscape**

Respondents were asked for their views on the evolution of the cyber threat landscape since the entry into force of the NIS Directive. An overwhelming majority of respondents indicated that the **cyber threat level has increased since 2016 (88.4%)**, with 43.7% believing it has significantly increased. Across different respondent categories there is a consensus that the cyber threat level has increased since 2016. The respondents on average rated SMEs as rather poorly prepared in dealing with the evolving cybersecurity threats.

Responses suggest that an increase in cybersecurity risk can notably be observed in the health sector, digital infrastructure, banking, electricity and financial market infrastructures. At the same time, respondents indicated that banking and financial market infrastructures hold the highest level of cybersecurity resilience. Conversely, the level of preparedness of the health sector was found lowest by respondents.

#### ✓ **Added value of EU security rules**

An overwhelming majority of the OPC respondents agreed that **common EU rules are needed to address cyber threats**. Two-thirds of them strongly agreed that cybersecurity rules should be aligned at EU level given that cyber risks can propagate across borders at high speed.

Just over half (56.3%) of the OPC respondents strongly agreed with the statement that mandatory sharing of cyber-risk related information between national competent authorities across the EU would contribute to a high level of joint situational awareness on cyber risks.

OPC respondents were less likely to disagree with the statement that all entities of a certain size providing essential services should be subject to similar EU-wide cybersecurity requirements (8.8% - 7.3% disagree, 1.5% strongly disagree).

#### ✓ **Sectorial scope of the NIS Directive**

Respondents were asked for their views about the appropriateness of the NIS Directive's sectoral coverage. The overall results revealed that OPC respondents on average show **significantly more support for the inclusion of public administrations and data centres within the scope of the NIS Directive**. Just over half of the respondents supported the coverage of the **chemicals (51.4%)** and **food supply (50.5%)** industries.

OPC respondents most frequently disagreed to the inclusion of social network providers (17.5%) and manufacturing industries (14.6%) in the scope of the Directive

Half of the OPC respondents believed that the scope of the NIS Directive should include **telecoms**, while 18% of the respondents were of the opposite view. The most frequent reasons given for including **undertakings providing public communications** were as follows (in order of importance): (i) OES are highly dependent on telecommunications; (ii) telecommunications are equivalent to essential services; they cover information transmission networks; (iii) telecommunications and data technologies are consolidating and facing similar threats (iv) necessity to harmonise standards horizontally to reduce legislative complexity, avoid loopholes and create a common culture of cybersecurity. Some variations could be observed among certain stakeholder categories. National competent authorities were more likely not to agree to include undertakings providing

public communications under the NIS scope. 71.4% of cyber professionals and 61.4% of OESs and DSPs held the opposite view.

Cyber professionals were more likely to agree to extend the scope of the NIS Directive to include further sectors and types of digital service at risk of cyber threats. On the other hand, OESs, DSPs and trade associations were far less likely to agree with 22.8% and 25% of them respectively disagreeing with the prospect of including further digital services within the scope of the NIS Directive.

Overall, the most frequently mentioned sectors in the respective open field questions were (in order of importance):

- Public services – e-government, e-health, and emergency services (police, fire)
- Telecommunications
- Energy and electricity
- Cloud and DNS providers
- Manufacturers of electronic hardware and software
- Traditional media online
- Social media platforms
- Postal and courier services
- Data centres
- Banking, finance, and insurance
- Food production and waste management

When asked about digital service providers, the most reported types services which respondents considered should be included in the NIS Directive were:

- Data centres
- Social media platforms (social networks)
- Manufacturers and suppliers of important hardware and software
- Providers of communication and navigation services
- Service hosting providers
- All digital or internet products and services
- Application service providers (SAAS) and stores
- Online collaboration environments/tools, including video conferencing
- ICT security services
- Outsourced services such as application maintenance, Third Applications Formula and testing: externalised management tests, and BPO: Business process Outsourcing
- OTT services
- Telecoms
- Managed service providers and Managed Security Services (MSS),
- Payment provider gateways and financial transactions sites

#### ✓ **Regulatory treatment of OESs and DSPs**

The respondents were asked to agree or not as to whether the "light-touch" regulatory approach applied towards DSPs is justified and therefore should be maintained. OPC respondents **more frequently believed that the "light-touch" regulatory approach applied to DSPs is no longer justified** and should not be maintained (39.8%) while almost of third of the respondents could not expressed an opinion on this issue. Conversely, only 27.7% of the OPC respondents thought the regulatory "light-touch" for DSPs should be maintained. Among the responding Digital Service Providers, however,

69.2% thought that the “light touch” regulatory approach should be maintained and only 23.1% that it should be done away with.

#### ✓ **National competent authorities and CSIRTs**

The respondents were asked to assess the extent to which the NIS Directive impacted national authorities dealing with the security of networks and information systems. Specifically, the question covered the following five components: (i) level of funding; (ii) level of staffing; (iii) level of expertise; (iv) cooperation of authorities across Member States; (v) cooperation between national competent authorities within Member States.

Results suggest a strong perceived impact of the NIS Directive with about every second respondent indicating a medium to high effect across all five areas. The share of those choosing low impact ranges between 7.3% and 9.7%. In the meantime, the portion of those finding the NIS Directive had no impact remains marginal (1.0%-1.9%) regarding funding, staffing and expertise. No respondent chose this answer option when it comes to aspects of cooperation.

Responses indicate a relatively strong perceived impact of the NIS Directive on national CSIRTs across the Member States. Nearly every second respondent considered that the Directive had high or medium impact across the six areas covered. In this regard, there appears to be no major discrepancies in response patterns. The Directive is found to have had the strongest impact regarding cooperation with OES and DSP. The share of those stating no impact is marginal, accounting for 0.5-1.5% of all answers.

#### ✓ **Identification of OESs and sector-specific aspects**

The respondents were asked about the effectiveness of the OES identification process. A **significant share of respondents finds that the current approach does not ensure that all relevant OES are identified across the Union** (37.4% disagrees and 6.3% strongly disagrees). In the same vein, above 40% of respondents disagree or strongly disagree with the statement that the identification process has contributed to the creation of a level playing field for companies from the same sector across the Member States.

On the other hand, it appears that there is a more positive view as for the active engagement of competent authorities with OES. Similarly, according to the majority of the respondents, OES are aware of their obligations under the NIS Directive.

A total of 115 OPC participants provided free-text answers. The most often discussed topic is the **lack of harmonised approach resulting in significant inconsistencies in the way that Member States draw up lists of OES**, divergent applications of the thresholds and different applications of the *lex specialis* principle. Companies of the same nature therefore might be imposed different requirements depending on the Member State where they operate. Likewise, a same company might be identified as OES in one Member State, a DSP in another Member State, or a service provider falling out of the NIS Directive in yet a different Member State. Existing convergence tools (i.e. Article 5(4) consultation procedure, and the NIS Cooperation Group working document on the identification of OES) have not been sufficiently used to achieve consistent identification of OES across the Union.

Analysing OPC responses concerning the scope of the NIS Directive related to essential services, the question of lowering identification thresholds appears to be most divisive with nearly equal share in favour and against.

The responses relating to the question of the identification of OESs point out that Member States’ approaches often show strong heterogeneity. To that end, it was suggested to set a common set of criteria to ensure a harmonised process of identification of OES.

The NIS Directive gives a wide room of discretion to Member States when it comes to the identification of operators of essential services, the setting of security requirements and the rules governing incident notification. Most respondents agreed that the approach leads to significant differences in the application of the Directive and has a **strong negative impact on the level playing field for companies in the internal market** (40.3%); the approach increases costs for OES operating in more than one Member State (48.1%); and that the approach allows Member States to take into account national specificities (52.9%).

Responses related to the context of OES identification refer to the **need to cover public sector** by the Directive considering the magnitude of data they treat and potential impacts of a cyberattack. These answers argue that every sector working with essential data like personal data or business data should be compliant with the NIS Directive. In particular, the public sector should be included in the scope of the Directive, and more specifically all emergency services (e.g. police, fire brigade, technical aid), public administrations (e.g. citizens' offices) as well as government offices at regional, state and federal level.

A handful of responses set out concrete (sub-)sectors to be covered by the NIS Directive. In light of the COVID-19 pandemic, the **pharmaceutical sector** has been identified.

Additionally, a small share of OPC answers link to the **transport sector**. According to these, **automobile industry** should be covered by the NIS Directive. Additionally, one response notes that transport (including rail, air, water) should differentiate between freight (referring to as critical) and passenger transport (referring to it as not critical). **Food supply** and **manufacturing** have also been mentioned by a few OPC participants.

#### ✓ SMEs

Responses suggest insufficient cyber resilience and risk management practices applied by SMEs. Particularly, **small companies appear to be most vulnerable** in this regard with 27% of respondents providing lowest-possible evaluation.

As far as small enterprises are concerned, 95 free-text answers have been received. Nearly all replies relate to the obstacles hindering their cybersecurity resilience. These argue that small companies often lack the financial and human capacity, staff and awareness to provide adequate cybersecurity to their operation. **A large share of small companies do not perceive cyber threats as a risk to them or find that they do not face the same level of risk presented by large or medium sized companies.** Answers note that the concern with a small company is when they have access into, or are connected with, larger targets, and thus become the vectors for cyber-attacks on more critical targets.

98 free-text answer have been received in relation to medium-sized companies. Issues discussed are strongly comparable to those mentioned in relation to small companies. These entities, although most often have some sort of cybersecurity strategy in place, lack sufficient capacity, technical, financial, and human) to develop cybersecurity capabilities matching increased threats and risks compared to those in relation to small enterprises.

There is an overall agreement that the level of resilience and risk management practices applied by SMEs differ from one sector to another. There appears to be an agreement that discrepancy exists related to level of resilience and the risk-management practices both by size of the enterprise and the (sub-) section in which it operates. These point out that in some sectors (i.e. banking, energy) there is a strong legislative framework and high level of cybersecurity maturity.



Many parties reflected their lack of knowledge or opinion on whether the exclusion of micro- and small enterprises from the scope of the NIS framework would be just, given their smaller impacts (38.8%). Objection to the statement came notably from cybersecurity professionals (of whom 42.9% disagreed or strongly disagreed with the sentiment), although this audience group in particular was starkly divided on the issue with almost half (47.6%) also taking the opposing stance. Trade associations and other stakeholders expressed greater support for the notion that micro-/small enterprise should be excluded from conventional treatment, however, with 42.6% and 30.6% of those asked agreeing or strongly agreeing, respectively.

Most of the OPC respondents (60.2%) either agreed or strongly agreed that European legislation should require Member States to put in place frameworks to raise awareness of cyber threats among SMEs and to support them in facing cyber threats. Only 5.8% of the respondents either disagreed or strongly disagreed.

#### ✓ **The NIS Directive's light-touch approach vis-à-vis DSPs**

Almost half (48.5%) of respondents asked about the effectiveness of the light-touch approach towards DSPs agreed that the **cross-border nature of the NIS Directive's operations justified the harmonised treatment of DSPs by comparison to OESs**. Much of the audience however (36.9%), expressed no overall stance on the matter. Amongst parties who objected most strongly to the statement that the approach was contextually justified were OESs and DSPs themselves (19.3% of whom disagreed or strongly disagreed), indicating that groups most affected by the approach may feel more negatively towards the NIS Directive's approach than those that are less impacted.

Opinions on whether national authorities' degree of supervision could be justified by the nature of services and cyber risk faced, in the case of DSPs, were divided. Over a third of respondents representing citizens (40.0%), cybersecurity professionals (42.9%) and national competent authorities (42.9%) disagreed or strongly disagreed with the statement, although among other groups, opinion was decidedly less negative. Trade association representatives, OESs and DSPs and other stakeholders generally perceived the justification of the level of national supervision to be more reasonable.

As regards the level of DSPs cyber resilience, overall, participants rated cloud computing services as being the most prepared when it comes to cybersecurity related risks (32.5% said high or very high), followed by online search engines (24.8%), and lastly online marketplaces (20.9%).

#### ✓ **Security requirements**

Most respondents thought that imposing security requirements on OES by the NIS Directive has high and medium impacts in terms of cyber resilience. This opinion was shared among all types of stakeholders, but especially among OESs & DSPs (43.9% and 36.8%) cybersecurity professionals (47.6% and 19%), and citizens (50% and 40%).

While respondents overall appreciate the security requirements brought by the NIS Directive, **lack of harmonisation limits its impact**. The impact might be lower for large organisations as there was already an incentive on companies to protect themselves. Impacts are different also across sectors and Member States. It was noted that most of the NIS requirements were already in place before NIS Directive, and adaptations had to be made on the incident reporting process.

Concerning the impact of imposing **security requirements on DSPs** by the NIS Directive, most stakeholders were not able to comment on the nature of the impact, including OESs & DSPs, Trade associations, NCAs & CSIRTs. However, those that did believed it had medium to high impact.

Overall, OPC respondents thought that DSP addressed in the NIS Directive were already aware of cybersecurity and had reasonable cyber security measures in place to protect their business models. Given the light-touch regime prescribed by the NIS Directive towards DSPs, the imposition of these minimal security requirements currently has a minimal impact on DSPs. The impact of imposing security requirements on DSPs also depends on the country. In countries where the maturity was initially low, the NIS had more impact.

Most stakeholders could not answer or disagreed with the statement that there is sufficient degree of alignment of security requirements for OES and DSPs in all Member States.

Respondents noted that while all Member States have introduced measures in accordance with the Directive so that OESs and DSPs have to have security requirements in place, improved alignment between the various approaches adopted in different Member States would be helpful because the wide discretion that is given to Member States under the NIS directive with respect to identifying OESs and establishing security requirements leads to incongruity between the different Member States.

The stakeholders were asked a series of questions on the different approaches of Member States towards security requirements. Most respondents agreed that: prescriptive requirements leave too little flexibility to companies (49%); prescriptive requirements make it difficult to take into account technological progress, new approaches to doing cybersecurity and other developments (48.1%); the different level of prescriptiveness of requirements increases a regulatory burden for companies operating across different national markets (44.7%); the companies should have the possibility to use certification to demonstrate compliance with the NIS security requirements (45.6%). Some respondents noted that a higher level of prescription that is outcome focused is required in order to create sufficient common understanding of what is the regulatory obligation, as well as in order to provide the necessary incentives to organizations to pursue that compliance.

#### ✓ **Incident notification**

Member States are required to ensure that entities notify the competent authority or the CSIRT of incidents having a significant impact on the continuity or provision of services. Stakeholders were asked about the implementation of notification requirements under the NIS Directive. Most respondents agreed that: different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES (39.8%); Member States have imposed notification requirements obliging companies to report all significant incidents (43.2%); and that the majority of companies have developed a good understanding of what constitutes an incident that has to be reported under the NIS Directive (41.3%). On the other hand, more stakeholders did not know (39.8%) or disagreed (31.6%) with the statement that the current approach ensures that OES across the Union face sufficiently similar incident notification requirements.

Respondents noted that since there are sometimes large differences in the definition of mandatory reporting of security incidents in the Member States, there are also **no uniform reporting obligations**. The lack of harmonisation for reporting of security incident under various regulations and programs, e.g. PSD2, GDPR, NIS, has led to a fragmented approach and creates an unnecessary compliance burden for OES. The lack of harmonization of incident reporting requirements at EU level is suggested an important issue. Identifying the right authority to inform and the right information to provide appears to be a heavy burden for firms along the critical path of managing the

incident itself. Fragmented approaches across Member States are suggested to imply additional regulatory and compliance burdens on companies.

The responding OESs and DSPs were overwhelmingly against the broadening of reporting obligations under the NIS Directive. This is also the case among the responding trade associations representing sectors both covered and not covered by the NISD. National competent authorities and cybersecurity professionals remain split on the issue.

As the OPC respondents were asked to think about ways of improving the information available to cybersecurity authorities on national level, they were then asked to describe which information gathered by national authorities should be made available at EU to improve common situational awareness. The most frequent information types given, in order of importance, were as follows:

- Aggregated statistical data describing the current cyber threat landscape.
- Top threats and top incidents in terms of occurrence.
- Emerging cyber threats.
- Incidents with cross-border relevance.
- Indicator of Compromise (IOC) notifications based on level of seriousness.
- Attacks on sectors, attack vectors, critical vulnerabilities.
- Best practices on risk identification, remediation and/or mitigation.

#### ✓ **Information sharing**

The respondents were asked to evaluate the level of incident-related information sharing between Member States. Setting aside those not in the position to reply, it appears that the level of information-sharing between MS requires substantial improvement as below chart presents. A larger proportion OPC respondents were critical than those assessing this aspect positively.

OPC respondents were also asked about ways in which organisations could be incentivised to share more information with cybersecurity authorities on a voluntary basis. The most frequent suggestions made by the respondents revolved around the **simplification of reporting processes** guaranteeing anonymity, as well as **free and transparent access to anonymised reporting information**.

The respondents were also asked to rate the level of information exchange on cybersecurity between organisations in their respective sectors. Around three-quarters of the respondents were unable to provide a rating. The level of information exchange was ranked the highest among organisations in the financial and banking sectors and the lowest among organisations in the health sector. A third of the respondents indicated a low level of information exchange across sectors, while a further 8.7% indicating a very low level. Just over a quarter of the respondents (26.7%) indicated a medium level of information exchange across sectors. Very few respondents thought the level of information exchange across sectors was high (3.4% or 7 out of 206 respondents).

The OPC respondents were then asked how the level of information exchange between companies could be improved within Member States but also across the European Union. The most frequent suggestions were made, in order of importance:

- Centralising the information sharing duties either at EU or national level.
- Greater role for CSIRTs: establishing trusted CSIRTs and encourage sectoral-level CSIRTs to foster national and international information-exchange.
- National boards of experts meeting regularly to exchange information and best practices on mitigation and remediation.
- Through structured and trust-based mechanisms ensuring anonymous information

sharing by competent authorities.

- Developing European-level ISACs at sectoral level.
- Industry-led initiatives for intra-sector information sharing between OES.
- Making it a legal obligation through an EU-level regulatory activity.
- Promote the use of robust, automated information sharing architectures, capable of turning threat indicators into security protections in near-real time.

#### ✓ **Enforcement**

Most respondents did not know or were unable to answer whether: Member States are effectively enforcing the compliance of OES (45.1%); Member States are effectively enforcing the compliance of DSPs (62.1%); the types and levels of penalties set by Member States are effective, proportionate and dissuasive (50.5%); and whether there is a sufficient degree of alignment of penalty levels between the different Member States (63.6%).

#### ✓ **Efficiency**

Most stakeholders agreed to some extent that **the effects of the NIS Directive have been achieved at a reasonable cost**. In particular, trade associations (42.6%, plus 7.4% to a large extent), OESs & DSPs (40.4%, plus 17.5% to a large extent), NCAs & CSIRTs (35.7%, plus 14.3% to a large extent), cybersecurity professionals (38.1%, plus 9.5% to a large extent), and citizens (50%). The majority of stakeholders thought that the **NIS Directive had medium to high impact on the overall level of resilience against cyber-threats across the EU**. This opinion was shared especially among the OES & DSPs (33.3% high impact and 38.6% medium impact), Trade associations (27.9% high impact and 27.9% medium impact), cybersecurity professionals (14.3% high impact and 38.1% medium impact) and citizens (20% high impact and (70% medium impact).

#### ✓ **Coherence with other legal instruments**

The majority of trade associations, OESs & DSPs, and citizens rated the **coherence of the NIS Directive** as being medium and high. On the other hand, most of cybersecurity professionals and NCAs & CSIRTs thought the coherence was low and very low.

#### ✓ **Vulnerability discovery and coordinated vulnerability disclosure**

The respondents were asked to evaluate the level of effectiveness of national policies that are making vulnerability information available in a timelier manner. Just under a quarter of the OPC respondents (24.8%) thought their level of effectiveness were medium, while 15.5% of the respondents rated the national disclosure policies as low or very low.

The OPC respondents were asked if their organisation have implemented a coordinated vulnerability disclosure policy. A significant proportion of the respondents did not respond or indicated this did not apply to them or their organisation (48%, 99 out of 206 respondents). 57 respondents went on to argue that national authorities such as CSIRTs could take proactive measures to discover vulnerabilities in ICT products and services provided by private companies.

## ANNEX 3: WHO IS AFFECTED AND HOW?

### 1. Practical implications of the initiative

The initiative would affect the following stakeholders:

- Private sector/industry
- Public administration (from the perspective of being included under the NIS scope)
- Competent authorities (including CSIRTs and SPOCs)

ENISA would also be affected in particular in policy option 3, which considers a number of additional measures within the limits of ENISA's mandate.

The assessment of impacts, including costs and benefits, for all the above-mentioned categories of stakeholders is covered by the main text of the Impact Assessment. This annex provides more detailed background information on the way the economic impact was analysed as regards the private sector/industry, for all the sectors, subsectors and services considered in the policy options, as well as public administration.

#### ➤ *Private sector/industry*

The NIS Directive is covering under its scope 7 sectors (each including subsectors and/or services) and types of digital services, as listed in Annexes II and III. In order to determine the potential impact of the policy options on businesses, the impact assessment considered the following steps:

- i. Determining the breadth of the (sub)sectors and services that would fall within the NIS scope, starting with the existing (sub)sectors and services, followed by the ones considered to be added in policy options 2 and 3.
- ii. Within these sectors, determining the extent of medium and large companies that would be covered under the NIS scope in policy option 3.
- iii. Estimating the average percentage of ICT security spending out of ICT spending and total revenue per sector and the likely evolution thereof.

Further, the impact assessment estimated the costs and benefits at the level of organisations, including the particular economic impact on SMEs, as also reflected in section 2 of this annex and then respective costs and benefits tables.

The data on the entities active in the (sub)sectors and services covered by or considered for the NIS scope are presented below in tables summarising the cross-sector estimates, as well as further below in a more detailed format, explaining the results presented in the summary tables. The analysis relied mainly on Eurostat and DESI data. Similar data was not available across the EU for all (sub)sectors or services analysed. Furthermore, the data was often available in aggregate forms which do not always entirely match the types of entities defined under the NIS scope, therefore in most cases the overall figures represent an overestimate. Whenever systematic data on number of companies and turnover was not available, proxies were used to the extent possible, including data or information on market structure or market shares. The data and estimates below provide therefore a meaningful, yet not comprehensive overview of the above-mentioned metrics. To the extent available, sector-specific data is provided on medium and large entities that would be covered as a rule by the NIS scope in policy option 3. Furthermore, for the sectors currently covered by the NIS scope, a comparison is being made with the number of OES notified by the Member States.

Mention should be made that in policy option 2, the identification process for OESs would be maintained. Even if a certain cross-sector harmonisation of identification of thresholds may be achieved, the overall identification system would remain complex and would not be expected to lead to a notable increase of identified OESs. Therefore, in this option, it is expected for competent authorities to supervise the same or a similar number of operators as the ones that are currently identified as OES rather than the total number of companies in the respective sectors and subsectors featured in the tables and supporting data below.

For all the data sourced Eurostat (notably number of companies, including medium and large, turnover and average turnover per company), the data used (as the most recent available) is from 2018. Where no source for the data/information is mentioned in the footnotes to the table, it shall be assumed that it is Eurostat data as mentioned above. The table cells marked N/A read as either no available data or not of application for that particular segment.

In relation to the following operators and service providers considered for the addition to the NIS scope due to their digital intensity, inter-dependencies with other sectors and/or importance for society (including in the light of the COVID-19 crisis), insufficient granular data was available to allow a data analysis in this Impact Assessment report: operators of government-owned and privately-owned ground-based infrastructure that support the provision of space-based services; EU reference laboratories (as defined by the Proposal for a Regulation of the European Parliament and of the Council on serious cross-border threats to health); manufacturers of medical devices and in vitro diagnostic medical devices (as defined in Regulation (EU) 2017/745 and Regulation (EU) 2017/746), manufacturers of medical devices considered as critical during a public health emergency (according to Article 20 of the Commission Proposal for a Regulation on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices); entities conducting research and development activities of medicinal products (as defined in Directive 2001/83/EC); electricity market participants as defined by Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined by Directive (EU) 2019/944, and operators of hydrogen production storage and transmission.

**Table 1: Cross-sector summary of the estimation of size and relevant turnover of the sectors, subsectors and types of services currently covered by the NIS framework – policy options 0, 2 and 3**

Sector or type of service	Subsector/s	Number of companies (EU level)	Number of companies of medium and large size (EU level)	Total turnover – million EUR (EU level)	Average turnover per medium and large company – million EUR (EU level)	Number of OES reported by Member States by October 2020 (EU level)	Comments/disclaimers
Energy	Electricity and gas supply	154,967	3,099	1,040,979.37	335.9	872	The data cover also energy generation companies, which are currently not in the NIS scope and are considered under policy options 2 and 3.
	Water	16,051	380	776,749.4	38.22	156	
Transport <sup>2</sup>	Air	4,172	228			165	For land transport, the NIS Directive covers only rail (infrastructure managers and railway undertakings) and road (road authorities and operators of intelligent transport services). For the road transport, data was not available to the level of granularity of the types of entities covered by the NIS framework. However, given that the
	Rail	Approx. 450 <sup>3</sup>	N/A			73	
	Road <sup>4</sup>	N/A	N/A			126	

<sup>2</sup> Of all transport sector, approx. 1.15% are of medium and large size.

<sup>3</sup> Assumption made based on Eurostat data from 2014-2018. No data was available on the medium and large rail enterprises.

<sup>4</sup> The NIS scope (Annex II of the NIS Directive) covers only road authorities and operators of intelligent transport services.

										NIS framework covers entities which are dependent on network and information system, it is unlikely that the number of such road transport entities would be high, rather in the ranges of hundreds.
Banking		6,088 <sup>5</sup>	Approx. 3,500 <sup>6</sup>	Assets of EUR 43,348B <sup>7</sup>	/	411				There was no available data on the overall revenues of banks in the EU.
Financial market infrastructure	CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs	350 <sup>8</sup>	N/A	N/A	N/A	172				There was no available data on the size of the market infrastructures, nor on their revenues.
Health	Hospitals	13,200 <sup>9</sup>	N/A	EUR 475,061.91 (expenditure) <sup>10</sup>	N/A	12,469 <sup>11</sup>				
Drinking	Water	14,116	870	EUR 49,082.8	28	822				These aggregated data are an overestimate,

<sup>5</sup> European Banking Federation data for 2019. It also includes the UK.

<sup>6</sup> Assumption made based using the banks which are covered by the system of European banking supervision as a proxy.

<sup>7</sup> <https://www.ebf.eu/facts-and-figures/statistical-annex/>.

<sup>8</sup> Impact assessment accompanying the review of the European Supervisory Authorities SWD(2017) 308

<sup>9</sup> 2.6 hospitals for 100,000 inhabitants estimated in Europe in 2015. Source: <https://hospitalhealthcare.com/latest-issue-2018/hope-2018/hospitals-in-europe-healthcare-data-9/>

<sup>10</sup> Healthcare expenditure in EU-27 was of EUR 1,309,016.26 million in 2018, while hospitals were the largest providers in expenditure terms, accounting for more than one third (36.3 %) of all expenditure in the EU-27: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare\\_expenditure\\_statistics#Healthcare\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare_expenditure_statistics#Healthcare_expenditure)

<sup>11</sup> Mention should be made that of this total 12,469, 10,897 entities were identified by a single Member State.



water supply and distribution	collection, treatment and supply								since, in addition to water supply, collection and treatment are also covered.
Digital infrastructure	Country-code top-level domain registries	28	28	major country-code top-level domain (ccTLD) <sup>12</sup>	28	N/A	N/A	173	Very limited market data is available for this sector.
	Individual internet exchange points (IXPs)	140	140	IXPs <sup>13</sup> (one company usually administers several IXPs)	N/A	N/A	N/A		

<sup>12</sup> one in each Member State plus EURid, which administers .eu

<sup>13</sup> Referenced for 2020. The 140 IXPs are located in the EU, with some being of global importance.

	Domain name system (DNS) providers - made up of a wide range of providers fulfilling different functions along the name resolution chain	Authoritative DNS Resolution	Two root name servers <sup>14</sup> , 28 major ccTLD entities <sup>15</sup> and a large number of domain name registrars and web hosting companies <sup>16</sup>	N/A	N/A	N/A	
		Recursive DNS Resolution	DNS resolvers provided by most internet service providers <sup>17</sup> and by third parties, mostly large global technology companies	N/A	N/A	N/A	

<sup>14</sup> providing authoritative DNS resolution for the root zone, located in the Netherlands and Sweden.

<sup>15</sup> The ccTLDs of the 27 Member States (such as .de, .fr or .pl) and of the European Union (.eu), but not counting regional ccTLDs, such as .ax of Åland Islands (Finland). These provide authoritative DNS resolution for their respective TLD namespaces.

<sup>16</sup> offering authoritative DNS resolution as part of their domain registration services.

<sup>17</sup> As part of the internet access arrangement. See the data on electronic communication networks and services.

Cloud computing services		Estimates of approx. 1,700 <sup>18</sup>	located outside the EU.	N/A	N/A	N/A	According to the 2020 Digital Economy and Society Index (DESI) <sup>23</sup> , in 2018, 26% of European enterprises purchased cloud computing services and incorporated cloud technologies. Among the enterprises that used cloud computing services, 55 % were 'highly dependent'. <sup>24</sup>  Telecoms are also often heavily featured in their local markets (e.g. Deutsche Telekom, Orange, KPN are among the main cloud providers). <sup>25</sup>  According to DESI <sup>26</sup> , across the EU market, total revenues generated by public cloud services increased by 21% between 2018 and 2019 and are expected to continue to grow
--------------------------	--	--	-------------------------	-----	-----	-----	--

<sup>18</sup> There is no precise estimate of the number of European cloud service providers, only estimates such as this one by business information platforms:

<sup>19</sup> <https://www.crunchbase.com/hub/europe-cloud-computing-companies>

<sup>20</sup> Oligopolistic market.

<sup>21</sup> France, Germany, the UK and the Netherlands.

<sup>22</sup> Salesforce, Rackspace and Oracle are global providers that are further down in the country rankings, with Salesforce ranking fifth overall across Europe.

<sup>23</sup> European players such as OVH, Enter, Aruba, Outscale and Fabasoft do not grasp any significant market shares globally.

<sup>24</sup> <https://ec.europa.eu/digital-single-market/en/integration-digital-technology>.

<sup>25</sup> At the two extremes, the majority of enterprises in the manufacturing sector (51 %) belonged to the upper-medium dependence group, while the majority in information and communication (71 %) reported using advanced services and hence belonged to the high dependence group.

<sup>26</sup> Among European telecoms, Deutsche Telekom is the largest cloud provider thanks to a strong position in Germany and smaller operations in multiple other countries, which help it to place sixth overall across all of Europe. Source: <https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries>

<sup>27</sup> <https://ec.europa.eu/digital-single-market/en/integration-digital-technology>

									by 50% until 2021.
Online marketplaces		7,000 <sup>27</sup>	120 <sup>28</sup>	357,203 <sup>29</sup>	N/A	N/A	N/A	N/A	By mid-2020, 1 million EU businesses were selling goods and services via online platforms. <sup>30</sup> In 2018, 40 % of EU enterprises with web sales used an e-commerce marketplace. <sup>31</sup> The number of users in e-commerce is expected to amount to 557.5m by 2024. The size of marketplaces varies widely, from turnover exceeding EUR 1 billion to a turnover of less than EUR 100,000. <sup>32</sup>
Online search engines		N/A	One dominant player (Google <sup>33</sup> ), followed by	N/A	N/A	N/A	N/A	N/A	

<sup>27</sup> Commission estimate of 2019: [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_1168](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168)

<sup>28</sup> Conservative estimate based on a sample of marketplaces for a competition-related sector inquiry conducted by the Commission in 2015-2017: REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report on the E-commerce Sector Inquiry, COM(2017) 229 final and SWD(2017) 154 final: [https://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_sw\\_d\\_en.pdf](https://ec.europa.eu/competition/antitrust/sector_inquiry_sw_d_en.pdf)

<sup>29</sup> Estimate of the revenue in the e-commerce market in Europe in 2020: <https://www.statista.com/outlook/243/102/ecommerce/europe>

<sup>30</sup> For 2017, the European Business-to-Consumer e-commerce turnover was forecasted to reach around EUR 602B, at a growth rate of nearly 14%.

<sup>31</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce\\_statistics#Web\\_sales\\_dominant\\_in\\_all\\_EU\\_countries](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics#Web_sales_dominant_in_all_EU_countries)

<sup>32</sup> REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report on the E-commerce Sector Inquiry, COM(2017) 229 final and SWD(2017) 154 final: [https://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_sw\\_d\\_en.pdf](https://ec.europa.eu/competition/antitrust/sector_inquiry_sw_d_en.pdf)

<sup>33</sup> Over 90% of the general search market in Europe.

						few small players <sup>34</sup>				
--	--	--	--	--	--	------------------------------------	--	--	--	--

---

<sup>34</sup> In the general search market in Europe, Google is the super dominant search engine with an estimated market share of over 90% of web searches (Netmarketshare.com.), followed by Bing with less than 3%. Players such as Seznam in Czechia and Qwant in France are among the very few European-based search engines present on this market.

**Table 2: Cross-sector summary of the estimation of size and relevant turnover for the additional sectors, subsectors and types of services considered for the extension of the NIS scope in policy options 2 and 3**

Sector or type of service	Subsector/s	Number of companies (EU level)	Number of companies of medium and large size (EU level)	Total turnover – million EUR (EU level)	Average turnover per medium and large company – million EUR (EU level)	Comments/disclaimers
Providers of electronic communications networks or of publicly available electronic communications services <sup>3536</sup>	Telecom providers	37,204	N/A	322,297	8.66 (for all sizes)	Both options 2 and 3 would cover all entities, irrespective of the size. For option 3, this represents an exemption from the size cap rule, due to the fact that this highly regulated sector already implements a high level of security standards and excluding micro and small providers from the NIS scope may negatively impact these existing standards.
	Programming and broadcaster providers	7,775	N/A	61,521.9	7.9 (for all sizes)	

<sup>35</sup> Broadcasting services are also considered under this sector, as well as emergency communication services

<sup>36</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information\\_and\\_communication\\_service\\_statistics\\_-\\_NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information_and_communication_service_statistics_-_NACE_Rev._2)

Chemicals and chemical products	Manufacturing	23,845	3,193	555,865.8	135.85	
Waste management	Waste collection, treatment and disposal activities	44,189	2,616	161,537.3	41.76	
Waste water	Sewerage	10,955	473	22,963.9	23	
Postal and courier services	N/A	89,480	869	102,036.2	69.87	
Food supply	Wholesale and retail sale of foods and beverages	595,233	5,303	1,056,828.1	98	The data represent an overestimate, since they also cover wholesale and retail of tobacco, which would not be included in the NIS scope in policy options 2 and 3.
Energy	Electricity generation	3,944 (representing at least 95% of the national net electricity generation in the EU)	82 main electricity generating companies <sup>37</sup>	N/A	N/A	The NIS Directive does not cover electricity generation under the electricity subsector. Policy options 2 and 3 would add this subsector to the NIS scope. The data on electricity generation companies (number and turnover) was included in the above aggregated data covering the

<sup>37</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity\\_generation\\_statistics\\_%E2%80%93\\_first\\_results#Production\\_of\\_electricity](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_generation_statistics_%E2%80%93_first_results#Production_of_electricity)





	operators (NEMOs)	N/A	N/A	N/A	N/A	The inclusion in the NIS scope of electricity market participants, as defined in point (25) of Article 2 of Regulation (EU) 2019/943, providing aggregation, demand response or energy storage services as defined in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944 providing aggregation, demand response or energy storage services was considered notably due to their importance for the energy sector and the Green Deal.
	Operators of hydrogen production and storage and transmission	N/A	N/A	N/A	N/A	No relevant granular data was available. The strategic vision for a climate-neutral EU envisages hydrogen as an important contributor to the EU energy mix by 2050 with a share of 13-14%. This position has been further fostered by the Communication “ <i>A hydrogen strategy for a climate-neutral Europe</i> ” COM(2020) 301). Turning clean hydrogen into a viable solution to a decarbonised EU will necessarily demand a dedicated infrastructure of key importance for the new EU energy

							system and economy in general. No relevant granular data was available.
Heat production and supply	District heating and cooling	N/A	N/A	672,000 (823,000 when biofuels and geothermal sectors are included) <sup>39</sup>	N/A	N/A	Heating and cooling accounts for approx. 46% of Europe's final energy demand. <sup>40</sup> In EU households, heating and hot water alone account for 79% of total final energy use. <sup>41</sup> Cooling is a fairly small share of total final energy use. In industry, 70.6% of energy consumption is used for space and industrial process heating, 26.7% for lighting and electrical processes such as machine motors, and 2.7% for cooling.
Health	EU reference laboratories	N/A	N/A	N/A	N/A	N/A	EU reference laboratories as defined in Article 15 of the Proposal for a Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU. No relevant granular data was available.

<sup>39</sup> considering biomass, biogas, heat pumps and solar-thermal segments.

<sup>40</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity\\_and\\_heat\\_statistics&oldid=493775#Derived\\_heat\\_production](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_and_heat_statistics&oldid=493775#Derived_heat_production)

<sup>41</sup> [https://ec.europa.eu/energy/topics/energy-efficiency/heating-and-cooling\\_en?redir=1](https://ec.europa.eu/energy/topics/energy-efficiency/heating-and-cooling_en?redir=1)

	Research and development activities of medicinal products as defined in Article 1 point 2 of Directive 2001/83/EC of the European Parliament and of the Council on the Community Code relating to medicinal products for human use.	N/A	N/A	N/A	N/A	N/A	N/A	Research and development activities of medicinal products as defined in Article 1 point 2 of Directive 2001/83/EC of the European Parliament and of the Council on the Community Code relating to medicinal products for human use. No relevant granular data was available.
Manufacturing	Food products	192,328	10,215	724,116.3	57.50			Given the breadth of the manufacturing sector, policy options 2 and 3 would consider the addition only of a number of manufacturing subsectors which would be of greater importance for the society and economies, taking also account of their relevance for the population and for the essential services currently covered by the NIS scope or considered to be added.
	Beverages	27,909	1,047	144,034.1	83.8			
	Basic pharmaceutical products and pharmaceutical preparations	3,352	934	240,420.3	224.46			This includes, among others, the manufacture of medicinal active substances to be used for their pharmacological properties in the manufacture of medicaments: antibiotics, basic vitamins, salicylic and O-acetylsalicylic acids, processing



									available.
Computer, electronic and optical products	33,063	2,410	279,521.2	104.2					
Electrical equipment	38,919	3,378	292,423.3	88.5					
Machinery and equipment	77,627	8,956	722,795.9	70.1					
Motor vehicles, trailers and semi-trailers <sup>42</sup>	16,585	2,944	1,106,882.1	369.85					
Other transport equipment	13,068	1,058	236,726.7	210.65					
Data centres	Geographically concentrated market in Europe	with Interxion, as Equinix or other market players,	N/A	N/A					Data centres provide different types of services enabling data processing and storage (such as colocation or dedicated hosting). Some large companies also operate their own data
Digital infrastructure									

<sup>42</sup> Very specific aspects relating to the manufacturing process of cars are also covered by the General Safety Regulation, notably reflecting the UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles. However, not all cybersecurity risks concerning the manufacturers are covered in that context, nor specific NIS-related requirements, such as incident reporting, information sharing, etc.

		Frankfurt, London, Amsterdam and Paris <sup>43</sup> dominating.	include global companies, but also medium and large firms focusing on the European market.				centres. Data centres are the physical infrastructure used for the provision of cloud-based services. The market is set to reach a size of approx. EUR 36.40 billion by 2025.
Content delivery networks (CDN)	Highly concentrated global market. None of the major providers are headquartered in the EU.	In 2016, 95 % of global CDN traffic for web-based apps was delivered by 10 companies.	N/A	N/A	N/A	N/A	N/A
Social networks	Very few social networks in Europe, most significant ones being non-European	Facebook had a market share in social media of over 70% and at times over 80% in 2019-2020, followed by	N/A	N/A	N/A	N/A	According to DESI <sup>45</sup> , 65% of internet users in the EU used social networks in 2019.

<sup>43</sup> So-called FLAP.

<sup>45</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Social\\_media\\_-\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_-_statistics_on_the_use_by_enterprises)

Trust service providers		businesses.	Pinterest, Twitter and Instagram with less than 12% and other players such as Youtube, Tumblr, Vkontakte with less than 1%. <sup>44</sup>				For this types of services, both options 2 and 3 would cover all entities, irrespective of the size. For option 3, this represents an exemption from the size cap rule, due to the fact that within the eIDAS framework, some security standards are already implemented and excluding micro and small providers from the NIS scope may negatively impact these existing standards.
Operators of government-owned and		190 active qualified trust service providers <sup>46</sup> operating in 28 of the 31 EU and EEA/EFTA countries <sup>47</sup>	N/A	N/A	N/A	N/A	Specific ground-based infrastructure that directly supports space-based components of the EU's space

<sup>44</sup> <https://gs.statcounter.com/social-media-stats/all/europe>

<sup>46</sup> There are further 19 trust service providers currently being taken over and further 59 without active trust services listed on the browser that comprise both the qualified and non-qualified status. D.4 – Draft Final Report, 14 September 2020 - *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation)*, SMART 2019/0046, Ecorys, VVA, Deloitte, Spark, pages 21-22 and 24.

<sup>47</sup> The European List of Trusted Lists (LOTL), sourced from the Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020.

privately-owned ground-based infrastructure that support the provision of space-based services						programme, including Galileo, EGNOS, Copernicus, GOVSATCOM and Space Surveillance and Tracking are excluded.  No relevant granular data was available.
--	--	--	--	--	--	--



Table 1 above is based on the following data and analysis.

### Energy

In the energy sector, the NIS Directive is currently covering:

- Electricity supply operators
- Electricity Transmission and Distribution System Operators
- Operators of oil transmission pipeline
- Operators of oil production, refining and treatment facilities, storage and transmission
- Gas supply operators
- Gas Transmission and Distribution System Operators
- Gas storage system operators
- LNG system operators
- Natural gas operators
- Operators of natural gas refining and treatment facilities

The data presented below covers the electric power generation, transmission and distribution subsector (*electricity supply subsector*), the manufacture of gas; distribution of gaseous fuels through mains subsector (*gas supply subsector*), as well as steam and air conditioning supply.<sup>48</sup> This data is presented in an aggregated form in Eurostat analysis. Although it does not fully match the scope of the entities covered by NIS under energy sector, it offer a meaningful proxy for the companies operating in the electricity and gas subsectors, which are covered by NIS. Of the above-mentioned aggregated data at EU level, steam and air conditioning supply represents only 5.15% of the number of companies and 2.52% of the overall turnover, which was then deducted from the total number of companies affected and corresponding turnover thereof.

Mention should be made that these aggregate data cover also energy generation companies, which are currently not covered by NIS and which are considered for the extension of the NIS scope under the policy options 2 and 3. The data is therefore an overestimate in this regard for the baseline scenario. Separate data only on electricity generation are presented under options 2 and 3 and the difference highlighted accordingly. There is no EU-wide Eurostat data available on the operators of oil transmission pipelines, oil production, refining and treatment facilities, storage and transmission.

According to the aggregate Eurostat data at EU level, the number of medium and large-size companies represent about 2% of the total number of companies in this sector.

---

<sup>48</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity,\\_gas,\\_steam\\_and\\_air\\_conditioning\\_supply\\_statistics\\_-\\_NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity,_gas,_steam_and_air_conditioning_supply_statistics_-_NACE_Rev._2)

Overview of number of affected businesses in the electricity and gas sector

	<i>Number of companies in electricity, gas, steam and air conditioning supply (2018)</i>	<i>Number of medium and large-size companies in electricity, gas, steam and air conditioning supply (2018)</i>
EU-27	163,125	1,492
<i>EU-27 total extrapolating data on number of medium and large size companies to deduct missing data from some MS<sup>49</sup></i>	/	3,262
<i>EU-27 total only electricity and gas (excluding the steam and air conditioning supply)</i>	154,967	3,099

Source: Eurostat<sup>50</sup>

By October 2020, Member States (EU-27) have notified to the Commission that they identified 872 OES in the energy sector.

The table below reflects the total turnover at EU level of companies in the electricity and gas subsectors in 2018:

*Estimation of average company turnover*

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL only electricity and gas for medium and large size enterprises (excluding the steam and air conditioning supply) (2018)</i>	<i>EU-27 TOTAL only electricity and gas for medium size enterprises (excluding the steam and air conditioning supply) (2018)</i>

<sup>49</sup> Taking account that overall, according to Eurostat data, approximately 2% of the total companies in electricity, gas, steam and air conditioning are of medium and large size.

<sup>50</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity, gas, steam and air conditioning supply statistics - NACE Rev. 2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity,_gas,_steam_and_air_conditioning_supply_statistics_-_NACE_Rev._2).

Turnover (million EUR)	1,450,460.3	1,067,890.2	1,040,979.37	137,890
Number of companies	163,125	3,262	3,099	974
Average turnover per company (million EUR)	/	/	335.9	141,57

Source: Eurostat<sup>51</sup>

### Transport

In the transport sector, the NIS Directive is currently covering:

- Air transport (air carriers, airport managing bodies, airports, entities operating ancillary installations contained within airports, traffic management control operators providing air traffic control).
- Rail transport (infrastructure managers, railway undertakings).
- Water transport (inland, sea and costal passenger and freight water transport companies, managing bodies of ports, operators of vessel traffic services).
- Road transport (road authorities, operators of intelligent transport systems).

*Overview of the number of companies, turnover and average turnover per company for land (rail, road) and transport via pipelines, water and air transport*

	<i>EU-27 TOTAL (2018) – land (rail, road) and transport via pipelines</i>	<i>EU-27 TOTAL for medium and large companies (2018) – land (rail, road) and transport via pipelines</i>	<i>EU-27 TOTAL (2018) – water</i>	<i>EU-27 TOTAL for medium and large companies (2018) – water</i>	<i>EU-27 TOTAL (2018) – air transport</i>	<i>EU-27 TOTAL for medium and large companies (2018) – air transport</i>	<i>EU-27 TOTAL (2018) – land, transport via pipelines, water and air</i>	<i>EU-27 TOTAL for medium and large companies (2018) – land, transport via pipelines water and air</i>
Turnover (million EUR)	548,085.4	304,630	122,979.1	45,046.5	105,684.9	46,592.3 (of which 8.089,2 for medium companies)	776,749.4	396,268.8
Number of companies	880,426	9,760	16,051	380	4,172	228 (of which 149 medium companies)	900,649	10,368
Average turnover per company	/	31.21	/	118.54	/	204.35 (of which 54,28 for medium companies)	/	38.22

<sup>51</sup> Idem.

(million EUR)								
---------------	--	--	--	--	--	--	--	--

Source: Eurostat<sup>52</sup>

The land transport category covered by the above table represents however an aggregate of a wide range of transport companies, ranging from rail to trucking industry, many of which are not actually covered by the NIS Directive, which in relation to land transport covers only: rail transport (in particular infrastructure managers and railway undertakings) and road (in particular road authorities, not covered by the land transport data, and operators of intelligent transport services, in relation to which it is unclear whether they are covered by the overall land transport data). The most recent and comprehensive data on the number of railway operators available in Eurostat dates from 2014: 435 operators. For the following years up to 2018, more data is missing per Member State, but nevertheless one could estimate, taking account of an average increase in the number of companies per Member State between 2014 and 2018, that the overall number of railway operators in 2018 in all Member States would be of about 450.<sup>53</sup> The number of medium and large operators would therefore be smaller. No data was available on the medium and large rail enterprises.

For the road transport, data by Eurostat or from other source was not available to the level of granularity of the types of entities covered by the NIS framework. However, given that the NIS framework covers entities which are dependent on network and information system, it is unlikely that the number of such road transport entities as defined by NIS would be high, rather in the ranges of hundreds, notably as regards medium and large entities.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 620 OES in the transport sector, of which 165 in the air transport, 156 in the water transport and 199 in land transport (73 rail and 126 road).

### Banking

European Banking Federation data shows that there were 6,088 banks in the EU (including UK) in 2019, with assets amounting to EUR 43,348B.<sup>54</sup> In the system of European banking supervision, banks are supervised by the European Central Bank and the national supervisors of the countries that participate in the system.<sup>55</sup> The banking supervision system covers 21 countries (of which four non-EU), 115 significant banks (representing 82% of euro area banking assets), under direct supervision of the European Central Bank, and 2,611 less significant banks, under direct national supervision. The significant and less significant banks covered by the European banking supervision system and amounting to 2,726, could be considered a proxy for medium and large size banks. While the European banking supervision system does not cover all EU Member States, it nevertheless covers a significant number thereof and information could be extrapolated as to assume that approximately 3,500 of credit institutions in the whole of the EU would be of medium and large size.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 411 OES in the banking sector.

<sup>52</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<sup>53</sup> [https://ec.europa.eu/eurostat/databrowser/view/rail\\_ec\\_ent/default/table?lang=en](https://ec.europa.eu/eurostat/databrowser/view/rail_ec_ent/default/table?lang=en)

<sup>54</sup> <https://www.ebf.eu/facts-and-figures/statistical-annex/>

<sup>55</sup> <https://www.bankingsupervision.europa.eu/about/ssmexplained/html/ssm.en.html>

There was no available data on the overall revenues of banks in the EU.

### Financial market infrastructures

The NIS Directive currently covers operators of trading venues and Central Counterparties.

The impact assessment accompanying the review of the European Supervisory Authorities<sup>56</sup> estimated around 350 market infrastructures (such as CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs) in the EU.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 172 OES in the financial market infrastructures.

There was no available data on the size of the market infrastructures, nor on their revenues.

### Health

The NIS Directive currently covers health care settings, including hospitals and private clinics.

Healthcare expenditure in EU-27 was of EUR 1,309,016.26 million in 2018.<sup>57</sup> Hospitals were the largest providers of healthcare in expenditure terms, accounting for more than one third (36.3 %) of all expenditure in the EU-27, i.e. EUR 475.061,91 million. Relative to population size and in euro terms, in 2017 the healthcare expenditure was highest among the EU Member States in Sweden (EUR 5,200 per inhabitant), Denmark and Luxembourg (both EUR 5,100 per inhabitant), with the lowest in Bulgaria (EUR 591 per inhabitant) and Romania (EUR 494 per inhabitant).<sup>58</sup>

There were 2.6 hospitals for 100,000 inhabitants estimated in Europe in 2015, i.e. approximately 13,200.<sup>59</sup>

By October 2020, Member States (EU-27) have notified to the Commission that they identified 12,469 OES in the health sector. The total number of hospitals cannot however be compared with the number of currently identified OES in the healthcare system (i.e.12,469). This is because about 87% of the number of identified OESs comes from the same Member State which identified every single hospital in the country, no matter the size, thus illustrating once more the deep divergence in the identification approaches at Member State level. In option 3, with the application of the size cap, this number is expected to considerably decrease. At the same time, additional medium and large hospitals in other Member States that currently were not identified as OES would be added in the NIS scope. The overall resulting number is however expected to be lower than the couple of thousand ranges.

### Drinking water supply and distribution

The NIS Directive currently covers suppliers and distributors of water intended for human consumption.

---

<sup>56</sup> SWD(2017) 308.

<sup>57</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare\\_expenditure\\_statistics#Healthcare\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare_expenditure_statistics#Healthcare_expenditure)

<sup>58</sup> Providers of ambulatory health care (25.6 %) and retailers and other providers of medical goods (17.6 %) were the second and third largest providers of healthcare in expenditure terms.

<sup>59</sup> <https://hospitalhealthcare.com/latest-issue-2018/hope-2018/hospitals-in-europe-healthcare-data-9/>

*Overview of the number of companies, turnover and average turnover per company for water collection, treatment and supply*

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>
Turnover (million EUR)	49,082.8	8,861.6	24,374.6
Number of companies	14,116	680	870
Average turnover per company (million EUR)	/	13	28

Source: Eurostat<sup>60</sup>

The above data is wider than the water supply subsector covered by the NIS Directive, therefore the overall number of companies and turnover would be a substantial overestimate.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 822 OES in the drinking water supply and distribution sector.

*Digital infrastructure*

As the NACE classification does not include separate categories for the various digital infrastructures covered by the NIS Directive and considered in the impact assessment, only very limited market data is available for this sector.

➤ *Country-code top-level domain registries*

In 2019 there were 28 major country-code top-level domain (ccTLD) registries with headquarters in the EU (one in each Member State plus EURid, which administers .eu). In 2019, all 28 entities were of medium or small size.

➤ *Internet exchange points*

In 2020 there were 140 individual internet exchange points (IXP) located in the European Union, with some being of global importance. The actual number of companies active in the sector is smaller, as companies often administer more than one IXP. While a small percentage of IXPs is managed by medium-sized companies, most IXPs in the EU are managed by small companies.

➤ *Domain name system providers*

The domain name system (DNS) is made up of a wide range of providers fulfilling different functions along the name resolution chain:

Authoritative DNS resolution:

- There are two root name servers, providing authoritative DNS resolution for the root zone, located in the Netherlands and Sweden.

<sup>60</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

- There are 28 major ccTLD entities<sup>61</sup> providing authoritative DNS resolution for their respective TLD namespaces.
- There is a large number of domain name registrars and web hosting companies offering authoritative DNS resolution as part of their domain registration services. These companies range from micro to large in size and many are located outside the European Union. For example, EURid lists 706 registrars for the .eu domain, of which 116 are located outside the EU.

Recursive DNS resolution:

- DNS resolvers provided by most internet service providers as part of the internet access arrangement (for numbers see section on electronic communication networks and services)
- DNS resolvers provided by third parties, mostly large global technology companies located outside the European Union.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 173 OES in the digital infrastructure sector.

### Cloud computing services

In 2018, the global cloud market<sup>62</sup> was estimated to account for USD 288B and is forecasted to grow by over 1.7 fold by 2021 to reach USD 475B<sup>63</sup>. While *public cloud* is and will remain the largest segment of the global cloud market with estimated revenues of USD 170B in 2018 and USD 277B by 2021, hybrid and private cloud will also grow. Total *hybrid cloud* revenues were estimated<sup>64</sup> to reach USD 52.2 B in 2018. By 2021, total revenues are expected to reach USD 79.5B. In 2018, total *private cloud* revenues were estimated<sup>65</sup> to reach USD 66.5B. By 2021, total private cloud revenues are expected to reach USD 99.9B. ‘*Software as a Service*’ (SaaS)<sup>66</sup> captures the two third of public cloud revenues while ‘*Infrastructure as a service*’ (IaaS)<sup>67</sup> and ‘*Platform as a Service*’ (PaaS)<sup>68</sup> respectively one fifth and one sixth. By 2021, SaaS will continue to capture more than half of the revenues, while IaaS and PaaS will double their respective revenues in average.

The public cloud market structure is oligopolistic composed of only few large companies in which the three leaders - AWS, Microsoft and Google - in aggregate account for

---

<sup>61</sup> The ccTLDs of the 27 Member States and .eu, but not counting regional ccTLDs, such as .ax of Åland Islands (Finland)

<sup>62</sup> Market growth *estimations are based on revenues generated from cloud delivery models – public, private and hybrid – for cloud service providers and IT operators.*

<sup>63</sup> *Worldwide Whole Cloud Forecast, 2017 – 2021, IDC, 2017.*

<sup>64</sup> *Worldwide Whole Cloud Forecast, 2017 - 2021, IDC, 2017.*

<sup>65</sup> *Worldwide Whole Cloud Forecast, 2017 - 2021, IDC, 2017.*

<sup>66</sup> instant computing infrastructure, provisioned and managed over the internet Examples: Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting.

<sup>67</sup> cloud computing model that provides virtualized computing resources over the internet. Examples: DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE).

<sup>68</sup> cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its own infrastructure. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift.

almost 65% of the market in 2018<sup>69</sup>. AWS is the leader. Alone it accounts for 40% of the public cloud market revenues when estimated by public IaaS and PaaS revenues. Microsoft and Google respectively rank second and third. Alibaba is the main key new entrant with already a strong presence in Asia.

Amazon remains the top cloud provider in Europe and the leader in all major European cloud country markets.<sup>70</sup> Microsoft ranks second, Google third and IBM fourth.<sup>71</sup> European players such as OVH, Enter, Aruba, Outscale and Fabasoft do not grasp any significant market shares globally. At European level, OVH (the largest European Cloud Service Provider) gets less than 1% of total revenues generated in this market. Telcos are often heavily featured in their local markets and Deutsche Telekom, Orange and KPN all rank fourth in their home countries. Among European telecoms, Deutsche Telekom is the largest cloud provider thanks to a strong position in Germany and smaller operations in multiple other countries, which help it to place sixth overall across all of Europe.<sup>72</sup> The table below provides an overview of the cloud services market in Europe for Q1 2020.

### Cloud Services Leadership – Europe

Rank	Total Europe	UK	Germany	France	Netherlands	Rest of Europe
Leader	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft
#3	Google	Google	Google	OVH	Google	Google
#4	IBM	IBM	Deutsche Telekom	Orange	KPN	IBM
#5	Salesforce	Rackspace	IBM	Google	IBM	Salesforce
#6	Deutsche Telekom	Salesforce	Oracle	IBM	Oracle	Swisscom

Based on IaaS, PaaS and hosted private cloud revenues in Q1 2020

Source: Synergy Research Group

While there is no precise estimate of the number of European cloud service providers (some business information platforms estimate over 1,700 cloud service providers in Europe)<sup>73</sup>, as mention above, only a handful appear to be of medium and large size and therefore would be under the NIS scope in policy option 3.

Overall, there are two expected future developments in the cloud market. First a significant raise in cloud demand for SaaS solutions that are tailored-made: (i) to respond to sectorial specific companies' needs, (ii) to enable emerging technology services to take-up such as AI and blockchain services and; (iii) to manage energy efficiently and secured data flows and workloads optimization across the entire computing continuum including at the edge. Second, a raise in the demand for both secured hybrid cloud and edge computing solutions associated with increased needs for system integration business products and skills and; change management competences along the computing value

<sup>69</sup> 'No Change at the Top as AWS Remains the Leading Public Cloud Providers in all Regions', Synergy Research Group, 2018.

<sup>70</sup> France, Germany, the UK and the Netherlands.

<sup>71</sup> Salesforce, Rackspace and Oracle are global providers that are further down in the country rankings, with Salesforce ranking fifth overall across Europe.

<sup>72</sup> <https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries>

<sup>73</sup> <https://www.crunchbase.com/hub/europe-cloud-computing-companies>



chain to support companies and public administrations' to successfully transition to hybrid cloud and efficiently utilizing edge computing.

The European cloud infrastructure service revenues (including IaaS, PaaS and hosted private cloud services) were USD 6B in Q1 2020, with trailing twelve-month revenues reaching well over USD 21B. They are currently growing at 38% per year. The four largest country markets are the UK, Germany, France and the Netherlands, which in aggregate account for 63% of the total. Other countries in the top ten are Italy, Spain, Ireland and Belgium. While much smaller than the US market, European cloud revenues are growing more rapidly.<sup>74</sup> Europe's public cloud market is however expected to grow at 22% until 2022.<sup>75</sup>

According to the Digital Economy and Society Index (DESI) thematic report on integration of digital technologies<sup>76</sup>, across the EU market, total revenues generated by public cloud services increased by 21% between 2018 and 2019. Total revenues are expected to continue to grow by 50% between 2019 and 2021. Software security, as a SaaS application, contributed €115.5 million to total SaaS revenues on the EU market. Its revenue growth rate is expected to increase by 48% between 2019 and 2021, making it the fastest growing SaaS application over that period.

### Online marketplaces

By mid-2020, 1 million EU businesses were selling goods and services via online platforms, and more than 50% of SMEs selling through online marketplaces sell cross-border. For 2017, the European Business-to-Consumer e-commerce turnover was forecasted to reach around EUR 602B, at a growth rate of nearly 14%.

Web sales can be carried out via own websites or apps or via e-commerce marketplaces available on external websites or apps. According to Eurostat data, during 2018, 88 % of EU enterprises with web sales used their own websites or apps, while 40 % used an e-commerce marketplace.<sup>77</sup> EU enterprises realised 7 % of their total turnover from web sales during 2018, where 6 % was realised from web sales via own websites or apps and only 1 % from sales via online marketplaces.

At global level, online marketplaces sold USD 2.03 trillion in 2019. Sales on marketplace sites, like those operated by Alibaba, Amazon, eBay and others, accounted for 57% of global web sales in 2019.<sup>78</sup>

According to Statista<sup>79</sup> the revenue in the e-commerce market in Europe is projected to reach USD 421,927m in 2020. The number of users in e-commerce is expected to amount to 557.5m by 2024. The average revenue per user is expected to amount to USD 877.33.

In 2019, the Commission estimated a number of approximately 7,000 marketplaces in the EU.<sup>80</sup> In a sector inquiry into e-commerce launched by the Commission in May 2015 and finalised in June 2017, 37 marketplaces were selected for the inquiry, including the most important marketplaces and price comparison tools in the EU at the time, both the biggest

---

<sup>74</sup> <https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries>

<sup>75</sup> International Data Corporation (IDC).

<sup>76</sup> <https://ec.europa.eu/digital-single-market/en/integration-digital-technology>

<sup>77</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce\\_statistics#Web\\_sales\\_dominant\\_in\\_all\\_EU\\_countries](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics#Web_sales_dominant_in_all_EU_countries)

<sup>78</sup> Digital Commerce 360's analysis:

<sup>79</sup> <https://www.statista.com/outlook/243/102/ecommerce/europe>

<sup>80</sup> [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_1168](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168)

international players and the most relevant regional ones, covering the sale and price comparison of all products within the scope of the sector inquiry.<sup>81</sup> The size of marketplaces varies widely and ranges from marketplaces with turnover exceeding EUR 1 billion to marketplaces with a turnover of less than EUR 100,000. The selected marketplaces targeted altogether customers in 14 Member States. It can therefore be considered that a conservative proxy for the number of large and medium online marketplaces active across all Member States could be roughly 120 marketplaces.

### Online search engines

In the general search market in Europe there is one super dominant search engine, Google, with an estimated market share of over 90% of web searches<sup>82</sup>, followed by Bing with less than 3%. European players such as Seznam in Czechia and Qwant in France are among the very few European-based search engines present on this market.

Table 2 above is based on the following data and analysis.

### Providers of electronic communications networks or of publicly available electronic communications services<sup>83</sup>

*Overview of number of telecommunication operators, turnover and average company turnover*

	<i>EU-27 TOTAL (2018)</i>
Turnover (million EUR)	322,297
Number of companies	37,204
Average turnover per company (million EUR)	8.66

Source: Eurostat<sup>84</sup>

*Overview of number of providers of programming and broadcasting activities, turnover and average company turnover*

	<i>EU-27 TOTAL (2018)</i>
Turnover (million EUR)	61,521.9
Number of companies	7,775
Average turnover per company (million EUR)	7.9

Source: Eurostat<sup>85</sup>

<sup>81</sup> REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report on the E-commerce Sector Inquiry, COM(2017) 229 final and SWD(2017) 154 final: [https://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_sw\\_d\\_en.pdf](https://ec.europa.eu/competition/antitrust/sector_inquiry_sw_d_en.pdf)

<sup>82</sup> Netmarketshare.com

<sup>83</sup> Broadcasting services and emergency communication services would also be included in this category.

<sup>84</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information\\_and\\_communication\\_service\\_statistics\\_-\\_NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information_and_communication_service_statistics_-_NACE_Rev._2)

### Chemicals (manufacture)

The production of chemicals hazardous to health in the EU was 222.6 million tonnes in 2018.<sup>86</sup> The aggregated production of chemicals hazardous to environment is of about 84 million tonnes.

*Overview of number of providers of manufacturing of chemicals, turnover and average company turnover*

	<i>EU-27 (2018)</i>	<i>TOTAL</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	555,865.8		433,797.5	105.238,9
Number of companies	23,845		3,193	2.422
Average turnover per company (million EUR)			135.85	43,45

Source: Eurostat<sup>87</sup>

### Digital infrastructure – Data centres

Data centres provide different types of services enabling data processing and storage (such as colocation or dedicated hosting). Some large companies also operate their own data centres. Data centres are the physical infrastructure used for the provision of cloud-based services. The European data centre market is geographically concentrated with Frankfurt, London, Amsterdam and Paris (so-called FLAP) dominating. It is set to reach a size of USD 43 billion by 2025. Market players, such as Equinix or Interxion, include global companies but also firms of medium and large size focusing on the European market.

### Digital infrastructure – Content delivery networks

Content delivery networks (CDN) operate on a highly concentrated global market. None of the major providers are headquartered in the European Union. In 2016, 95% of global CDN traffic for web-based apps was delivered by only 10 companies. In 2019, the 10 biggest providers by number of customers were of large size.

### Waste management

*Overview of the number of companies, turnover and average turnover per company for waste collection, treatment and disposal activities; materials recovery*

---

<sup>85</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information\\_and\\_communication\\_service\\_statistics\\_-\\_NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information_and_communication_service_statistics_-_NACE_Rev._2)

<sup>86</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Chemicals\\_production\\_and\\_consumption\\_statistics#Production\\_of\\_chemicals\\_hazardous\\_to\\_the\\_environment](https://ec.europa.eu/eurostat/statistics-explained/index.php/Chemicals_production_and_consumption_statistics#Production_of_chemicals_hazardous_to_the_environment)

<sup>87</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	161,537.3	109,256.4	36.829,5
Number of companies	44,189	2,616	2.152
Average turnover per company (million EUR)	/	41.76	17.11

Source: Eurostat<sup>88</sup>

### Wastewater

Overview of the number of companies, turnover and average turnover per company for the sewerage subsector

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	22,963.9	10,880.7	4.929,3
Number of companies	10,955	473	408
Average turnover per company (million EUR)	/	23	12

Source: Eurostat<sup>89</sup>

### Manufacturing

Other than the manufacturing of chemicals and chemical products, which was also covered separately above, the *manufacturing subsectors considered in policy options 2 and 3 and their respective size and turnover are included in the table below.*

<sup>88</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<sup>89</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<i>Manufacturing subsectors</i>	<i>Number of companies (2018)</i>	<i>Number of companies of medium and large size (2018)</i>	<i>Total turnover – million EUR (2018)</i>	<i>Total turnover for companies of medium and large size – million EUR (2018)</i>	<i>Average turnover per company of medium or large size – million EUR (2018)</i>
Food products	192,328	10,215 (of which 8.149 medium companies)	724,116.3	587,440 (of which 189.078,6 for medium companies)	57.50 (23.2 for medium companies)
Beverages	27,909	1,047 (of which 813 medium companies)	144,034.1	87,748.1 (of which 23,157.2 for medium companies)	83.8 (28.48 for medium companies)
Basic pharmaceutical products and pharmaceutical preparations	3,352	934 (of which 538 medium companies)	240,420.3	209,649.6 (of which 14,802.3 for medium companies)	224.46 (27.51 for medium companies)
Computer, electronic and optical products	33,063	2,410 (of which 1,786 medium companies)	279,521.2	251,145.4 (of which 43.496,5 for medium companies)	104.2 (24.35 for medium companies)
Electrical equipment	38,919	3,378 (of which 2,425 medium companies)	292,423.3	298,973.1 (of which 49,072.7 for medium companies)	88.5 (20.23 for medium companies)
Machinery and equipment	77,627	8,956 (of which 7,053 medium companies)	722,795.9	627,831.8 (of which 145,420.4 for medium companies)	70.1 (20.61 for medium companies)

Motor vehicles, trailers and semi-trailers	16,585	2,944 (of which 1,771 medium companies)	1,106,882.1	1,088,852 (of which 42,646.2 for medium companies)	369.85 (24.08 for medium companies)
Other transport equipment	13,068	1,058 (of which 739 medium companies)	236,726.7	222,876.3 (of which 15.512,3 for medium companies)	210.65 (21 for medium companies)

Source: Eurostat<sup>90</sup>

### Postal and courier services

Overview of the number of companies, turnover and average turnover per company in the postal and courier activities subsectors

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	102,036.2	60,717.9	3,238
Number of companies	89,480	869	621
Average turnover per company (million EUR)	/	69.87	5.21

Eurostat<sup>91</sup>

### Food supply

In policy options 2 and 3 food supply would be added to the NIS scope, and in particular the subsectors of wholesale and retail sale of foods and beverages.

Overview of the number of companies, turnover and average turnover per company for wholesale and retail of food, beverages and tobacco

	<i>EU-27 TOTAL (2018) – wholesale</i>	<i>EU-27 TOTAL for medium and large companies (2018) – wholesale</i>	<i>EU-27 TOTAL (2018) – retail</i>	<i>EU-27 TOTAL for medium and large companies (2018) – retail</i>	<i>EU-27 TOTAL (2018) – wholesale and retail</i>	<i>EU-27 TOTAL for medium and large companies (2018) – wholesale and retail</i>

<sup>90</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<sup>91</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

Turnover (million EUR)	924,834.3	501,698.5	131,993.8	18,200.6	1,056,828.1	519,900 (of which 217.427,5 for medium companies)
Number of companies	188,146	4,352	407.087	951	595,233	5,303 (of which 4,593 medium)
Average turnover per company (million EUR)	/	115.27	/	19.14	/	98 (47.33 for medium companies)

Source: Eurostat<sup>92</sup>

The above data represent an overestimate since they also cover wholesale and retail of tobacco, which would not be included under NIS scope in policy options 2 and 3.

New energy subsectors and/or operators

- *Electricity generation*

The data on electricity generation companies (number and turnover) was included in the above aggregated data covering the electricity and gas subsectors.

In 2018, there were 3,944 generating companies representing at least 95% of the national net electricity generation in the EU and 82 main electricity generating companies.<sup>93</sup>

By October 2020, Member States (EU-27) have notified to the Commission that they identified 473 OES in the electricity subsector, excluding electricity generation. There was no granular data available on number of medium and large electricity generation companies.

- *Central oil stockholding entities*

Under the Oil Stocks Directive (2009/119/EC), Member States must maintain emergency stocks of crude oil and/or petroleum products equal to at least 90 days of net imports or 61 days of consumption, whichever is higher. Member States may meet this stockholding obligation in different ways. Emergency stocks can be held by the Member State itself or through so-called Central Stockholding Entities (CSEs) set up for this purpose in the form of a non-profit making body or service; the Member State may also impose an obligation on economic operators (typically oil companies) to hold the stocks for the benefit of the State. Several Member States have opted for a mixed system where part of the stocks is held by economic operators while the other part is held by a Central Stockholding Entity.

<sup>92</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do/>

<sup>93</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity\\_generation\\_statistics\\_%E2%80%93\\_first\\_results#Production\\_of\\_electricity](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_generation_statistics_%E2%80%93_first_results#Production_of_electricity)

The most centralised systems are those in which one organisation (the CSE usually established by the State), is the sole organisation responsible for holding emergency stocks. The most decentralised model is a model in which the entire stockholding obligation is put on the economic operators in the oil industry (and consequently no CSE exists), while the intermediate model is one in which the stockholding obligation is divided between industry and the CSE.

There are 23 Central Stockholding Entities in the European Union. Four Member States currently have no CSE, placing the entire obligation on the industry: Greece, Malta, Romania and Sweden. Two Member States, albeit having established a CSE, put the obligation almost exclusively on industry: Italy and Luxembourg.

- *(Nominated) Electricity market operator*

A nominated electricity market operator' or 'NEMO' means a market operator designated by the competent authority to carry out tasks related to single day-ahead or single intraday coupling, as defined in point (8) of Article 2 of the Regulation on the internal market for electricity (EU) 2019/943. An 'electricity market operator' means an entity that provides a service whereby the offers to sell electricity are matched with bids to buy electricity, as defined in point (7) of Article 2 of the Regulation on the internal market for electricity (EU) 2019/943.

The energy market highly depends on trading platforms and are thus crucial for the market. These trading platforms rely on IT systems.

There are approx. 16 NEMOs in Europe. Some Member States have/used to have only one NEMO: AT (EXAA); BG (IBEX); Croatia (CROPEX), CZ (OTE); GR (HENEX); HU (HUPX); Ireland (EirGrid); IT (GME); PL (TGE); PT (OMIE); RO (OPCOM); SK (OKTE); SI (BSP);. In other Member States the two main players are EPEX and Nordpool, with also the new entrant Nasdaq present in some of them.

NEMOs are often small companies. EPEX is one of the biggest NEMO and has 200 employees.

- *Electricity market participants engaged in aggregation, demand response or energy storage services*

Electricity market participant engaged in aggregation, demand response or energy storage services means a natural or legal person who is engaged in aggregation or who is an operator of demand response or energy storage services, including through the placing of orders to trade, in one or more electricity markets, including in balancing energy markets, as defined in point (25) of Article 2 of Regulation on the internal market for electricity (EU) 2019/943.<sup>94</sup>

Aggregation, storage and demand response increase the flexibility in energy markets and are highly needed elements, which are evolving very rapidly and will increase in numbers.

These categories of services within the energy sector are developing and are an important part of the implementation of the Green Deal. All these categories of services rely heavily on IT and OT as there is a need to respond to real time signals.

---

<sup>94</sup> this definition refers only to market operators dealing with aggregation, demand response services, energy storage.



### Heat production and supply

There were no granular data available on the number of companies and turnover in the heat production and supply sector in the EU. Some estimates indicate a turnover of the heating and cooling industry (considering biomass, biogas, heat pumps and solar-thermal segments) of EUR 67.2 billion and EUR 82.3 billion when biofuels and geothermal sectors are included.

### Social networks

According to DESI<sup>95</sup>, social networks (51 %) were the most used form of social media platforms in 2019. Furthermore, 65% of internet users in the EU used social networks in 2019.<sup>96</sup> In Europe, the social media platforms players are very few. Facebook had a market share in social media of over 70% and at times over 80% in 2019-2020, followed by Pinterest, Twitter and Instagram with less than 12% and other players such as Youtube, Tumblr, Vkontakte with less than 1%.<sup>97</sup>

### Trust service providers

The European List of Trusted Lists (LOTL) comprises all of the trusted lists managed by Member States within the scope of the Regulation (e.g. eSignatures, eSeals, WA, eTimestamps, ERDs, eSeal creation devices, eSignature creation devices, preservation service/archive). The Trusted List Browser developed by the European Commission<sup>98</sup> covers all trust service providers established in the European Union or in Norway, Liechtenstein or Iceland.

According the LOTL<sup>99</sup>, there are currently 190 active qualified trust service providers operating in 28 of the 31 EU and EEA/EFTA countries. There are a further 19 trust service providers currently being taken over and a further 59 trust service providers without active trust services listed on the browser that comprise of both the qualified and non-qualified status.<sup>100</sup>

The draft final report of the *Evaluation study of the eIDAS Regulation*<sup>101</sup> notes that qualified eSignatures are the services provided most on the market, followed by qualified time stamps and qualified eSeals. Out of the core trust services<sup>102</sup>, the qualified electronic registered delivery service is the most limited one, with 20 active services in seven Member States. The market offering of qualified website authentication certificates is additionally relatively lower than the offering for qualified eSignatures, qualified eSeals and qualified time stamps, which is likely due to the market being highly concentrated<sup>103</sup>.

---

<sup>95</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Social\\_media\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_statistics_on_the_use_by_enterprises)

<sup>96</sup> <https://ec.europa.eu/digital-single-market/en/use-internet>

<sup>97</sup> <https://gs.statcounter.com/social-media-stats/all/europe>

<sup>98</sup> <https://webgate.ec.europa.eu/tl-browser/#/>

<sup>99</sup> Sourced from the Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020.

<sup>100</sup> D.4 – Draft Final Report, 14 September 2020 - *Evaluation study of the Regulation no. 910/2014 (eIDAS Regulation)*, SMART 2019/0046, Ecorys, VVA, Deloitte, Spark, pages 21-22 and 24.

<sup>101</sup> Idem.

<sup>102</sup> Qualified certificate for electronic signature, Qualified certificate for electronic seal, Qualified time stamp, Qualified certificate for website authentication, Qualified electronic registered delivery service.

<sup>103</sup> ENISA, 2015, Qualified Website Authentication Certificates.

*Preliminary data on number of active qualified trust services in Europe<sup>104</sup>*

Qualified certificate for electronic signature	152	28	AT, BE, BG, HR, CY, CZ, EE, FI, FR, DE, EL, HU, IS, IE, IT, LI, LT, LV, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES
Qualified time stamp	109	23	AT, BE, BG, HR, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified certificate for electronic seal	102	24	AT, BE, BG, HR, CY, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified certificate for website authentication	51	20	AT, BE, BG, HR, CZ, FI, FR, DE, EL, HU, IT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified electronic registered delivery service	20	7	BE, FR, DE, NL, PL, SI, ES
Qualified validation service for qualified electronic signature	15	10	BE, BG, CZ, FR, LT, PL, SI, SK, ES, SE
Qualified validation service for qualified electronic seal	15	10	BE, BG, CZ, FR, LT, PL, SK, SI, ES, SE
Qualified preservation service for qualified electronic seal	13	9	BG, CZ, FR, HU, MT, PL, RO, SK, ES
Qualified preservation service for	12	7	BG, CZ, FR, HU, MT, PL, RO, SK, ES

<sup>104</sup> Statistics sourced from Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020.

qualified electronic signature			
--------------------------------------	--	--	--

Source: Draft Final Report, 14 September 2020 - Evaluation study of the Regulation no.910/2014 (eIDAS Regulation), SMART 2019/0046, Ecorys, VVA, Deloitte, Spark

Member States may add trust services other than qualified ones to the Trusted List on a voluntary basis.

A study that looked into the uptake of eIDAS services by SMEs found a generally low level of awareness of eIDAS solutions among SMEs: only 17% of SMEs had used an eIDAS solution already in their business.<sup>105</sup>

➤ **Public administration (from the perspective of being included under the NIS scope)**

In policy options 2 and 3, the NIS framework would only cover under ‘public administration’ central governments (i.e. all administrative departments of the state and other central agencies whose responsibilities cover the whole economic territory of a country), as well as the major socio-economic regions (104 in total according to the Nomenclature of territorial units for statistics–NUTS 2021 classification) and the basic regions for the application of regional policies (283 in total according to the NUTS 2021 classification).<sup>106</sup>

No attempt was made however for estimating the number of individual public institutions since the objective of the cost assessment is to make a global estimate of the total cost for the public sector. Data for the public administration relate to the operating costs. ICT spending in the public sector is typically expressed as a percentage of the operating expenditure instead of revenues or turnover.<sup>107</sup>

According to Eurostat<sup>108</sup>, in 2019, the total expenditure at **central government** level in the EU-27 was of 22% of GDP. The total revenue was of 21.7% of the GDP. At the **local government** level, the total expenditure was the same as the total revenue: 10.9% of the GDP. The composition of total government expenditure is reflected in the table below:

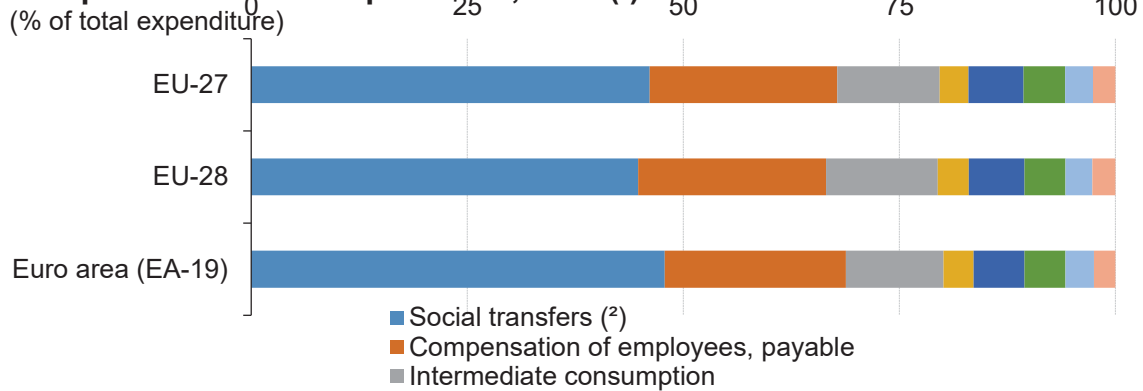
<sup>105</sup> eIDAS Study on pilots for replication of multipliers: supporting the uptake of eIDAS services by SMEs, SMART 2016/ 0084. See publication here: <https://op.europa.eu/en/publication-detail/-/publication/0627f219-5044-11e9-a8ed-01aa75ed71a1/language-en>.

<sup>106</sup> <https://ec.europa.eu/eurostat/web/regions/background>.

<sup>107</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Total\\_general\\_government\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Total_general_government_expenditure)

<sup>108</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government\\_finance\\_statistics](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_finance_statistics)

### Composition of total expenditure, 2019 <sup>(1)</sup>



<sup>(1)</sup> Data extracted on 22.04.2020.

<sup>(2)</sup> Social benefits other than social transfers in kind and social transfers in kind - purchased market production.

Source: Eurostat (online data code: gov\_10a\_main), Government finance statistics<sup>109</sup>

### ***Estimating the percentage of ICT security spending out of ICT spending and total revenue and evolution thereof of the sectors, subsectors and types of services currently covered and to be covered by NIS in the preferred option***

There is no available data to measure the actual impact of the NIS Directive on the level of ICT security spending for the companies activating in the sectors and subsectors or providing services under the NIS scope. Given the above-mentioned lacunae in comparable economic data, the analyses of economic impact and efficiency under all policy options, including the baseline scenario, would refer to widely accepted qualitative indicators for assessing the costs and benefits of various cybersecurity measures, along the lines described above, as well as a number of illustrative examples of tools used for this purpose and outcome thereof.

In the Impact Assessment that supported the proposal for the NIS Directive<sup>110</sup>, the level of **investment in IT security** was estimated on the basis of Gartner's global IT key metrics which indicated a percentage of IT security expenditure per sector out of the total revenue. The global ICT security spending data were estimated for 2012 and ranged between 3.04% to 6.61% of the total ICT spending per sector (with lowest in transport and healthcare, and highest in energy and digital infrastructure, including telecoms), while the ICT spending ranged between 1.10% and 7.60% of the total turnover per sector (with lowest in the energy sector and the highest in the banking and financial sector, as well as digital infrastructure sector and telecoms). One could therefore assume that, at global level, the ICT security spending at the time was in average about 5% of the ICT spending per sector and ICT spending was in average 4.3% of the total turnover, therefore leading to an average ICT security spending of about 0.215% of the total turnover.

The corresponding updated granular data were not available to the Commission at the time of the writing of this impact assessment report. However, while analysing Gartner press releases on their regular forecasts of the percentage of global IT security spending out of the total revenues, one could see the overall evolution of **ICT security spending and ICT spending** over the years. Thus, the estimated increases of ICT security spending

<sup>109</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government\\_finance\\_statistics#Government\\_revenue\\_and\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_finance_statistics#Government_revenue_and_expenditure)

<sup>110</sup> SWD(2013) 32 final.

at global level out of ICT spending were from USD 65.9 billion in 2013<sup>111</sup>; to USD 123.8 billion in 2020 (i.e. an average growth of 82.83% from 2013 to 2020)<sup>112</sup>, while the evolution of ICT spending was estimated from USD 2.69 trillion in 2013<sup>113</sup> to USD 3.56 trillion in 2020 (taking account a conservative scenario that assumes a post-COVID-19 recession)<sup>114</sup>, i.e. an increase of 32.34% from 2013 to 2020.

Some sectors or services would indeed have a more significant or faster growth of ICT security investment than others. For example, according to Gartner estimates and forecast, **8 of 10 cybersecurity markets are projected to grow faster than the market average, with cloud security growing the fastest.** Cloud security is the smallest, fastest-growing cybersecurity market segment with market size of USD 439 million in 2019, with a projected growth of 33% growth in 2020 up to USD 585M, mainly due to its small initial market size and organizations' preference for cloud-based cybersecurity solutions.<sup>115</sup>

In the banking sector, a survey by Deloitte and FS-ISAC<sup>116</sup>, referred to in the Impact Assessment for the Digital Resilience Act for financial services<sup>117</sup>, shows that on average banks, insurers, investment management firms and other financial services companies spend between 6% and 14% of their IT budget on cybersecurity, with an average of 10%. These account to a range of between 0.2% and 0.9% of the total revenues, with an average of about 0.3%. The above-mentioned impact assessment stresses that, while it is impossible to estimate the recurring costs of a general improvement of qualitative ICT risk requirements, it could be estimated that bringing ICT requirements up to a decent standard for all financial institutions would mean that institutions which have spending below the average would have to bring this up to the average. Another survey by Deutsche Bank<sup>118</sup> provides a breakdown on how much of the IT spending is dedicated to cyber security by financial institutions. On average, around 10% of financial institutions are below the 6%-14% range mentioned above.

Considering the above-mentioned overall evolution of global ICT spending and ICT security spending, one could assume for the purposes of this impact assessment that the average ICT security spending per sector would be in 2020 of approx. 9.14% of the ICT spending per sector. Depending on the level of cybersecurity maturity and capabilities of the sector, an adjustment of +/-3% could be made to this average. As for the overall ICT spending per sector, the average would be of approx. 5.69% of the total turnover. Depending on the level of digitalisation of the sector, an adjustment of +/-3% could be made to this average. This would entail an ICT security spending of approximately 0.52% of the total turnover. These extrapolations indeed do not reflect the precise differences in ICT and ICT security spending between sectors, which can be considerable, therefore it may be an overestimate for some and an underestimate for some others, however, overall, it may offer a conservative calculation basis which can help estimate to a certain extent

---

<sup>111</sup> <https://www.gartner.com/en/newsroom/press-releases/2014-08-22-gartner-says-worldwide-information-security-spending-will-grow-almost-8-percent-in-2014-as-organizations-become-more-threat-aware>

<sup>112</sup> <https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem>

<sup>113</sup> <https://www.gartner.com/en/documents/2601718>

<sup>114</sup> <https://www.gartner.com/en/documents/3982876>

<sup>115</sup> <https://www.forbes.com/sites/louiscolumbus/2020/08/09/cybersecurity-spending-to-reach-123b-in-2020/#766ad2a0705f>.

<sup>116</sup> <https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>.

<sup>117</sup> SWD(2020) 203 final, p.43.

<sup>118</sup> [https://www.db.com/newsroom\\_news/Deutsche\\_Bank\\_Investor\\_Report.pdf](https://www.db.com/newsroom_news/Deutsche_Bank_Investor_Report.pdf)

the weight of ICT security spending in the turnover of entities covered or considered to be covered in the future by NIS.

The overall global ICT security spending<sup>119</sup> increased with approximately 22% from 2017 (the year after the entry into force of the NIS Directive) and 2020. While this increase is not directly linked to the NIS Directive, one can assume nevertheless that it also integrates the spending generated by security requirements such as those provided by NIS which largely follow international standards. Therefore, assuming that in the medium-term (three to four years), the **new sectors** to be added to the NIS scope would entail **about 22% increase in their ICT security spending** would be a conservative assumption, most likely an overestimate, since it would consider a premise where the only trigger for extra IT security investment in these sectors and services would be the NIS framework. Yet, many other factors would naturally contribute to such increase, such as evolution of technologies and threat landscape, GDPR and other regulatory obligations, effects of particular incidents that may occur in the meantime or major crises, level of awareness, level of digitalisation, etc.

**For the sectors currently covered by the NIS Directive**, one would rather expect a more limited increase of ICT spending in the coming three to four years, slightly over (+4-5%) the pace of ICT security spending increase forecasted by Gartner in December 2019, prior to the COVID-19 crisis: i.e. **about 12% increase**.<sup>120</sup>

## 2. Summary of costs and benefits

The tables below present the costs and benefits which have been identified and analysed during the impact assessment process.

(1) *Estimates are relative to the baseline for the preferred option as a whole (i.e. the impact of individual actions/obligations of the preferred option are aggregated together); (2) The comment section indicates which stakeholder group is the main recipient of the benefit.*

<b><i>I. Overview of Benefits (total for all provisions) – Preferred Option</i></b>		
<b><i>Description</i></b>	<b><i>Amount</i></b>	<b><i>Stakeholder group main recipient of the benefits</i></b>
<b><i>Direct benefits</i></b>		
Reduce administrative burden by discarding the identification process	n/a	<ul style="list-style-type: none"> <li>• national authorities</li> <li>• businesses</li> </ul>
More clarity and further harmonisation would allow more focus on core cybersecurity tasks	n/a	<ul style="list-style-type: none"> <li>• national authorities</li> </ul>
Increase in compliance with security requirements	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>

<sup>119</sup> <https://www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/>

<sup>120</sup> <https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem>

		<ul style="list-style-type: none"> <li>• national authorities</li> </ul>
Single entry point for notifications concerning security breaches stemming from the NIS Directive, the General Data Protection Regulation and the ePrivacy Directive reducing administrative burden stemming from reporting obligations	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>
Decrease in cybercrime losses (medium/long term by implementing higher level of security requirements)	Use of higher level of security requirements and in particular fully deployed security automation (e.g. use of advanced technology, AI, automated scanning tools, etc) help companies reduce the lifecycle of a breach by 74 days compared to companies with no security automation deployment, from 308 to 234 days.	<ul style="list-style-type: none"> <li>• businesses</li> <li>• citizens</li> </ul>
Decrease in security incidents and cybercrime losses	Estimated reduction in cost of cyber incidents by EUR 11.3 billion over a 10-year period	<ul style="list-style-type: none"> <li>• businesses</li> <li>• citizens</li> </ul>
Reduction in cost liability for breaches	n/a	<ul style="list-style-type: none"> <li>• businesses</li> <li>• citizens</li> </ul>
Increase of trust of customers	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>
Protection from unfair competition (e.g. by avoiding industrial espionage)	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>
Increased and consistent level of resilience at the level of key businesses and cross-sector	n/a	<ul style="list-style-type: none"> <li>• businesses</li> <li>• national authorities</li> <li>• citizens</li> </ul>
Improved situational awareness	n/a	<ul style="list-style-type: none"> <li>• businesses</li> <li>• national authorities</li> <li>• citizens</li> </ul>

Increased operational capabilities	n/a	<ul style="list-style-type: none"> <li>• national authorities</li> </ul>
<i>Indirect benefits</i>		
Improved personal data protection	n/a	<ul style="list-style-type: none"> <li>• citizens</li> </ul>



**II. Overview of costs – Preferred option**

		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
<b>Action (a)</b> <i>Extension of the NIS scope (including adding a size cap)</i>	Direct costs	n/a	n/a	<p>Average increase in ICT security spending for the new sectors/services added to the NIS scope in the next 3-4 years.</p> <p>For the new sectors or services, an increase of about 25% of ICT spending could be expected for medium enterprises.</p> <p>Note: overall, in addition to the estimated increase in ICT spending triggered by the extension of the sectorial scope, an</p>	<p>Costs of implementation of higher security requirements and documented security measures</p>	<p>Personnel and administrative costs leading to an overall increase of approx. 20-30% of resources of the relevant authorities per Member State at central level mainly needed for performing supervisory actions and interactions with industry (including sector-specific)</p>	<p>Regular personnel and enforcement costs</p>

				<p>average 12% increase in ICT security spending is estimated for the sectors/services currently under the scope of the NIS Directive scope in the next 3-4 years. For medium enterprises, this estimate is of approx. 15%. This increase concern the cumulative effect of all measures envisaged by the preferred option.</p>			
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
<p><b>Action (b)</b> <i>Discarding the identification process and putting all operators and digital service providers under an equal footing, while</i></p>	Direct costs	n/a	n/a	Negligible personnel costs (notably legal departments), no additional FTE	n/a	n/a	n/a
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a

<p><i>differentiating on importance/criticality grounds</i></p> <p><b>Action (c)</b> <i>Further harmonising and streamlining risk management/security requirements</i></p>	<p>n/a</p>	<p>n/a</p>	<ul style="list-style-type: none"> <li>• Personnel (including potentially setting up new in-house teams): 2 -4 extra FTEs</li> <li>• Administrative costs</li> <li>• Opportunity costs</li> <li>• Potential increase in purchase costs on cybersecurity of +10-15%.</li> </ul>	<ul style="list-style-type: none"> <li>• Purchase costs (consultancy, audit, penetration tests, etc.)</li> </ul>	<p>Approx. 20-30% increase in budget/expenses), same increase as triggered by supervisory and enforcement-related measures + administrative costs for the sector-specific decentralised models for the new sectors/services to be added to the NIS scope</p>	<p>Recurrent personnel and technical costs (audits, testing, etc).</p>
<p>Direct costs</p>	<p>n/a</p>	<p>n/a</p>	<p>n/a</p>	<p>n/a</p>	<p>n/a</p>	<p>n/a</p>
<p>Indirect costs</p>	<p>Potential increase in prices of products as a result of investment in cybersecurity technologies and measures</p>	<p>n/a</p>	<p>n/a</p>	<p>n/a</p>	<p>n/a</p>	<p>n/a</p>

<b>Action (d)</b> <i>Security elements concerning supplier relationships and supplier-specific risk assessment</i>	Direct costs	n/a	n/a	<ul style="list-style-type: none"> <li>Personnel - in average 1 FTE</li> <li>Purchase costs (consultancy, audit)</li> <li>Opportunity costs</li> </ul>	<ul style="list-style-type: none"> <li>Personnel and potential regular outsourcing for risk assessments (notably for SMEs); potential increase of 2-4% in recurrent purchase ICT security costs</li> </ul>	<ul style="list-style-type: none"> <li>Part of the overall 20-30% increase in budget/expenses triggered by the extended NIS scope, further harmonisation of security requirements and enhanced supervisory activities.</li> <li>1-2 FTEs (legal and technical background)</li> </ul>	Regular personnel costs
		Potential slight increase in prices of products as a result of investment in cybersecurity technologies and measures	n/a	n/a	n/a	n/a	n/a
<b>Action (e)</b> <i>Streamlining incident notifications</i>	Direct costs	n/a	n/a	Personnel costs - potentially 1-2 FTE/organisation	Regular personnel costs	Personnel costs (1-2 potential software purchase of reporting summary of incident reports to ENISA)	Regular personnel costs
		n/a	Potential slight increase in prices of products as a result of investment in cybersecurity technologies and measures	n/a	n/a	n/a	n/a

	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (f)</b> <i>Reinforcing and further harmonising and supervision and enforcement</i>	Indirect costs	n/a	Personnel (2FTE/organisation) and purchase costs (in particular for DSPs and SMEs)	n/a	Regular personnel costs and potential increase in outsourcing, notably for audits (in particular for SMEs and DSPs) – overall additional 5% of recurrent purchase costs	n/a	Part of the overall 20-30% increase in budget/expenses) + administrative costs for the sector-specific decentralised models for the new sectors/services to be added to the NIS scope + 1-2 additional FTEs per competent authority	n/a	Personnel Purchase costs Administrative costs	n/a		
	Direct costs	n/a										
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (g)</b> <i>Incentivising the increase in Member States resources for and prioritising of cybersecurity policies (e.g. peer review and mutual assistance</i>	Indirect costs	n/a										
	Direct costs	n/a	n/a	n/a	n/a	n/a	For the mutual assistance mechanism: 2-3 FTEs per CSIRT team) For the peer-review:	Personnel and costs triggered by operational activities – in average 5,000 EUR per year per authority for peer-review missions – partially supported				

<i>mechanism)</i>								by the EU's Digital Europe Programme
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (h)</b> <i>Strengthening and cooperation sharing (including through ISACs with public authorities participation)</i>	Direct costs	Personnel costs – 1 extra FTE/organisation	Personnel costs – 1	More involvement in the public-private partnerships and ISACs – recurrent personnel costs ( <i>medium level</i> )	Personnel costs – 1-2 FTEs	Regular personnel costs		
	Indirect costs							
<b>Action (i)</b> <i>Incentivising coordinated vulnerability disclosure</i>	Direct costs		Negligible personnel costs (could, use existing FTEs who would monitor an additional input channel)	Negligible personnel costs	<ul style="list-style-type: none"> <li>Part of the overall 20-30% increase in budget/expenses triggered by the extended NIS scope, further harmonisation of security requirements and enhanced supervisory activities.</li> <li>Personnel (1/2 FTEs)</li> <li>Administrative costs</li> </ul>	Regular personnel and purchase/maintenance costs		



#### **ANNEX 4: METHODOLOGY AND CRITERIA FOR DETERMINING THE ADDITIONAL SECTORS, SUBSECTORS AND SERVICES CONSIDERED FOR THE NIS SCOPE IN POLICY OPTIONS 2 AND 3**

The additional sectors, subsectors and services were chosen based on:

- (i). the Member States' policy choices to go beyond the scope of the NIS Directive at national level.

The Commission's Report on OES identification<sup>121</sup> revealed that, at the time of the report, 11 out of 28 Member States have identified essential services in sectors not falling under the scope of Annex II of the NIS Directive. Out of these, 7 have identified a total of 157 OES providing services not covered by the types of entities in Annex II. This is illustrated by the table below.

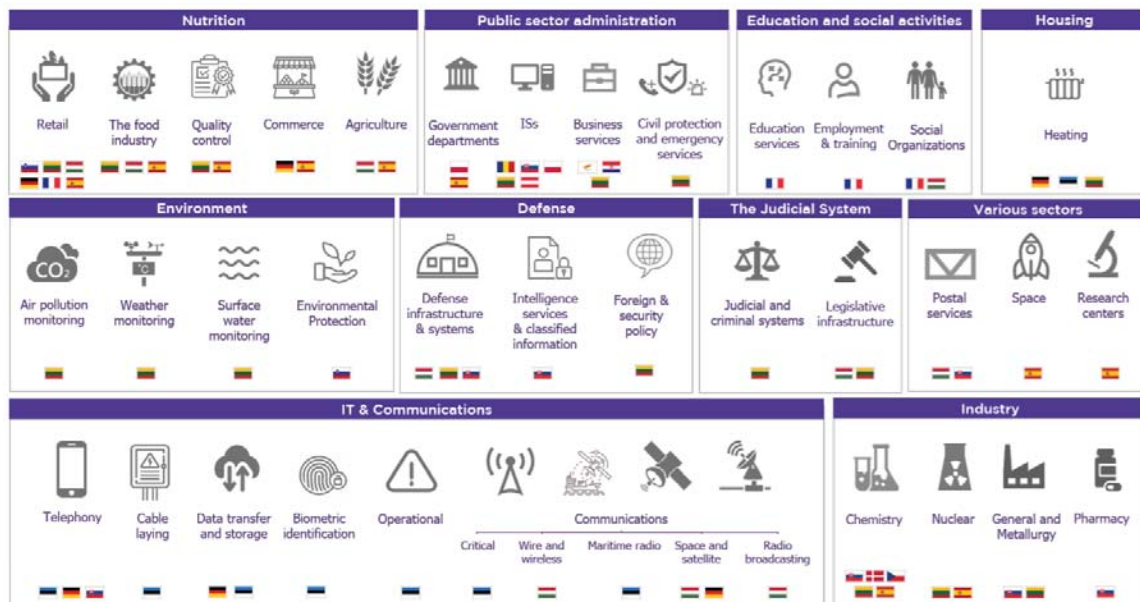
<b>Additional sector</b>	<b>Examples of entities</b>	<b>Number of Member States</b>
Information infrastructures	Data centres, server farms	5
Financial services (entities not listed in Annex II)	Insurance and reinsurance companies	4
Government services	Electronic services for citizens	4
Heat	Heat producers and suppliers	3
Wastewater	Collection and treatment facilities	3
Logistics	Postal services	2
Food	Producers, trading venues	2
Environment	Disposal of hazardous waste	2
National security/emergency services	112, crisis management	2
Chemical industry	Suppliers and producers of substances	2
Social services	Entities in charge of social benefits	1
Education	Authorities in charge of national exams	1
Collective catering	Distribution management	1
Water	Hydraulic structures	1

In a recent study on the transposition of the NIS Directive, Wavestone (2019)<sup>122</sup> shows that more than half of the Members States have added about 15 subsectors that are not covered by the scope of the NIS Directive.

<sup>121</sup> European Commission (2019), REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems. From now on the "OES Report".

<sup>122</sup> Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665 – implemented by Wavestone, CEPS and ICF.





Source: Wavestone, The NIS Directive, An Overview of Transposition In Europe For Operators Of Essential Services (OESs), June 2020

(ii).stakeholders’ views reflected in the results of the OPC and NIS review study surveys.

The OPC and the NIS review study surveys inquired about the potential addition of sectors in which essential services are being provided.

As regards the sectors and subsectors concerning OES:

➤ The results of the OPC were as follows:

<i>Sectors for operators of essential services</i>	<i>Strongly agree + agree to include the sector in scope of the NIS Directive [%]</i>
Public administration	70.8%
Food supply	50.5%
Manufacturing	46.1%
Chemicals	51.5%
Waste water	51.9%
Data centres	68.9%

Furthermore, 50% of the OPC respondents considered that ‘*undertakings providing public communications networks or publicly available electronic communications services currently covered by the security and notification requirements of the EU framework on electronic communication networks and services will be included in the scope of the NIS Directive*’.

- The results of the surveys conducted within the NIS study were as follows:
  - the response from competent authorities is illustrated in the table below

<i>Sectors for operators of essential services</i>	<i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i>
Insurance and reinsurance	35%
Chemicals	42%
Manufacturing	32%
Trust services	35%
Food supply	58%
Public Administration	68%
Elections (authorities, technology and process)	48%
Electricity generation	77%
Post and other delivery services	45%
Data centres and Content Delivery Networks (CDN)	65%
Heat production and supply	55%
Wastewater	58%
Waste management	48%
Emergency services	61%
Broadcasting services	52%

- the response from OESs is illustrated in the table below

<i>Sectors for operators of essential services</i>	<i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i>
Insurance and reinsurance	42%
Chemicals	50%
Manufacturing	50%
Trust services	58%
Food supply	67%
Public Administration	67%
Elections (authorities, technology and process)	50%

Electricity generation	83%
Post and other delivery services	50%
Data centres and Content Delivery Networks (CDN)	83%
Heat production and supply	50%
Wastewater	67%
Waste management	58%
Emergency services	58%
Broadcasting services	50%

Other sectors and subsectors mentioned by over 10% of the respondents to both OPC and NIS review study surveys:

<b>Other sectors mentioned by the respondents to the OPC and the targeted surveys of the NIS study</b>	<b>%</b>
Wastewater treatment	19% of respondent competent authorities
Energy generation	13% of respondent competent authorities

The results of the surveys conducted within the NIS review study were as follows:

- the response from competent authorities is illustrated in the table below:

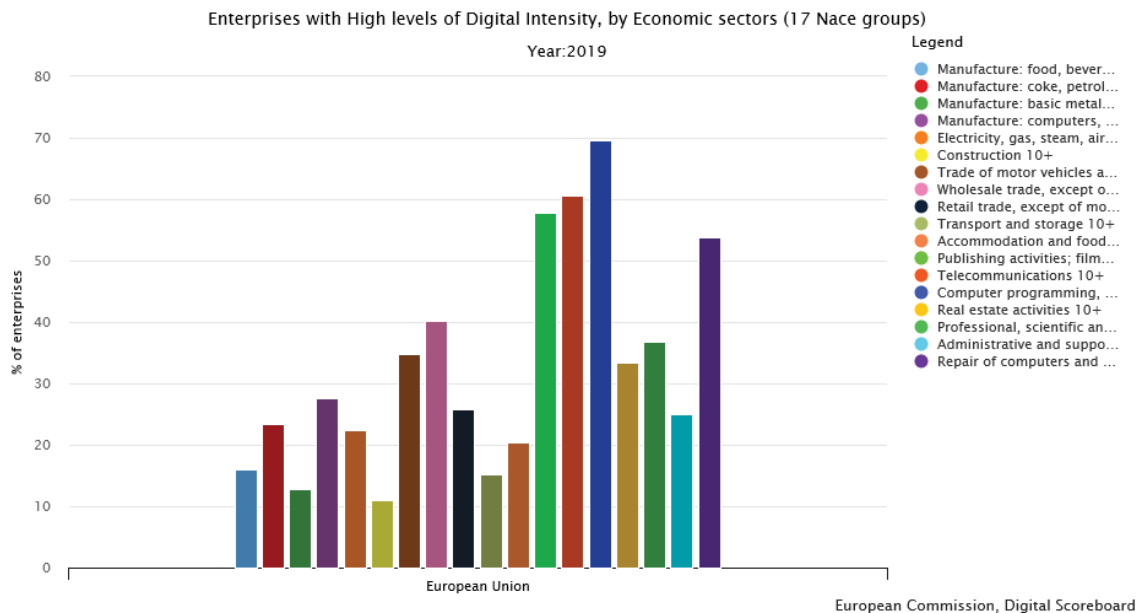
<b>Potential new DSPs</b>	<b><i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i></b>
Geolocation services	86%
Social networks	50%
Data centres and content delivery networks	86%

- the response from DSPs is illustrated in the table below:

<b>Potential new DSPs</b>	<b><i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i></b>
Geolocation services	100%
Social networks	100%
Data centres and content delivery	100%

## (iii). sectorial digital intensity

The 2019 data on digital intensity by economic sector of the Digital Economy and Society Index (DESI) was assessed to determine the digital-intensity levels of certain sectors.<sup>123</sup>



Furthermore, the taxonomy of sectors by digital-intensity developed by the OECD in 2018 was also analysed, with the caveats and limitations mentioned further below.<sup>124</sup> See also the following illustrative chart:

<sup>123</sup> [https://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={"indicator-group":"ebusiness","indicator":"e\\_di\\_hivhi","breakdown-group":"econsector","unit-measure":"pc\\_ent","time-period":"2019","ref-area":\["EU"\]}](https://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={)

<sup>124</sup> OECD, (2018), A taxonomy of digital intensive sectors”, OECD Science, Technology and Industry Working Papers, No. 2018/14, OECD Publishing, Paris, <https://doi.org/10.1787/f404736a-en>. This taxonomy was built using data from 2001-2015 for 36 sectors in 12 OECD countries to create ad hoc indicators. The sectors are classified according to ISIC Rev 4 and the indicators considered were: ICT equipment and software investment relative to fixed investment; intensity in purchase of ICT intermediate goods and services relative to output; stock of robots per employee; number of ICT specialists over total employment and propensity to engage in e-commerce sales.

Taxonomy of sectors by digital-intensity, overall ranking, 2013-15

ISIC Rev.4 industry denomination	Quartile intensity	ISIC Rev.4 industry denomination	Quartile intensity
Agriculture, forestry, fishing	Low	Wholesale and retail trade, repair	Medium-high
Mining and quarrying	Low	Transportation and storage	Low
Food products, beverages and tobacco	Low	Accommodation and food service activities	Low
Textiles, wearing apparel, leather	Medium-low	Publishing, audiovisual and broadcasting	Medium-high
Wood and paper products, and printing	Medium-high	Telecommunications	High
Coke and refined petroleum products	Medium-low	IT and other information services	High
Chemicals and chemical products	Medium-low	Finance and insurance	High
Pharmaceutical products	Medium-low	Real estate	Low
Rubber and plastics products	Medium-low	Legal and accounting activities, etc.	High
Basic metals and fabricated metal products	Medium-low	Scientific research and development	High
Computer, electronic, optical products	Medium-high	Advertising and other business services	High
Electrical equipment	Medium-high	Administrative and support service	High
Machinery and equipment n.e.c.	Medium-high	Public administration and defence	Medium-high
Transport equipment	High	Education	Medium-low
Furniture; other manufacturing; repairs	Medium-high	Human health activities	Medium-low
Electricity, gas, steam and air cond.	Low	Residential care and social work activities	Medium-low
Water supply; sewerage, waste	Low	Arts, entertainment and recreation	Medium-high
Construction	Low	Other service activities	High

Source: Calvino et al. (2018) based on Annual National Accounts, STAN, ICIO, PIAAC, International Federation of Robotics, World Bank, Eurostat Digital Economy and Society Statistics, national Labour Force Surveys, US CPS, INTAN-Invest and other national sources.

However, the above-mentioned index also has its limitations, having been built with data dating back to 2015. Therefore, it does not take into account, for instance, the profound digital transformation of certain sectors due to the increasing use of IoT and AI.















- (iv). level of importance for society of sectors, subsectors and services revealed by major crisis and in particular COVID-19

To complement the above-mentioned factors, consideration was also given to the role the sectors, subsectors and services have played during the COVID-19 crisis. The unprecedented nature and scale of this crisis stressed once more the criticality of sectors such as healthcare, which faced an increasing level of cyber threats, while at the same time revealed the importance for society of other sectors, such as food distribution and supply, in spite of these not showing a high degree of connectivity with other sectors. The analysis of this criterion was therefore mainly a qualitative one, taking account of the national authorities' decisions to qualify certain sectors or types of services as essential for society during the imposition of restrictive measures aimed at reducing the spread of the COVID-19 pandemic.

- (v). interdependency among sectors, notably in regard of digital infrastructures and DSPs

For this criterion, ENISA's assessment of the interdependencies between the OESs and DSPs was considered<sup>125</sup>. The figure below illustrates ENISA's conclusions with regard to dependencies among OES and DSPs.

<sup>125</sup> *Good practices on interdependencies between OES and DSPs*, ENISA, November 2018: <https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps>

OPERATOR OF ESSENTIAL SERVICES			DIGITAL SERVICE PROVIDERS		
Sector	Subsector		Online marketplace 	Online search engine 	Cloud computing service 
 Energy	Electricity 		●	●	●
	Oil 		●	●	●
	Gas 		●	●	●
 Transport	Air Transport 		●	●	●
	Rail Transport 		●	●	●
	Water Transport 		●	●	●
	Road Transport 		●	●	●
Drinking water supply and distribution			●	●	●
Digital infrastructure			●	●	●

● Low ● Medium ● Medium-High

Source: ENISA - Dependencies of Operators of Essential Services on Digital Service Providers (overview)<sup>126</sup>

Based on the above-mentioned criteria, a scoring from 0 to 2 per criterion was attributed to each of the potentially new sectors, subsectors and services, as follows:

- on the Member States’ policy choices to go beyond the scope of the NIS Directive at national level – a score of 0 if no Member State added the sector/subsector/service, 1 if 1 or 2 Member States added that sector, 2 if 3 Member States or more added it.
- on the stakeholders’ views reflected in the results of the OPC and/or in the targeted surveys for competent authorities, OES and DSPs:
  - 0 if less than 35% of the OPC respondents agreed or strongly agreed and/or, in the case of the targeted consultations of the NIS review study, if 35% and fewer of the median of the two relevant categories (i.e. competent authorities and operators of essential services or competent authorities and digital service providers) of responding stakeholders agreed to some extent, a moderate extent or a great extent;
  - 1 if between 35 and 50% of the OPC respondents agreed or strongly agreed and/or, in the case of targeted consultations of the NIS review study, if between 35% and 50% of the median of the three categories (or, as applicable, two categories) of responding stakeholders agreed to some extent, a moderate extent or a great extent;

<sup>126</sup> Figure 4, page 14 of ENISA’s *Good practices on interdependencies between OES and DSPs*, November 2018.

- 2 if over 50% of the OPC respondents agreed or strongly agreed and/or, in the case of targeted consultations of the NIS review study, if over 50% of the median of the three categories (or, as applicable, two categories) of responding stakeholders agreed to some extent, a moderate extent or a great extent.
- on sectorial digital intensity, DESI and the OECD data were cumulatively considered: 0 for low, 1 for medium-low and medium 2 for medium-high and high. For sectors where several subsectors were highlighted in the sources mentioned above, an average score for the overall sector was considered. For sectors and services not covered by the above-mentioned indexes, reasonable assumptions were made.
- on the level of importance for society of sectors, subsectors and services revealed by major crisis and in particular COVID-19: 0 for very little to no importance; 1 for relative importance and 2 for high importance;
- on interdependency among sectors, notably in regard of digital infrastructures and DSPs and exposure to cybersecurity risks: 0 for low to no level of reliance of other sectors/subsectors on the given sector/subsector and impact of potential threats; 1 to relative level and 2 for high level.

The sectors, subsectors and services totalling **5 points or higher out of the total of 10**. These results are marked in the table below.

Geolocation services, while they scored sufficiently high to be considered for the NIS scope, notably due to the high scores in the consultations and surveys, were eventually not considered for any of the policy options. This is because it was not possible to define with sufficient precision the type of providers or sectors these would belong to.

In addition to the sectors, subsectors and services subject to the NIS review consultations mentioned above and reflected in the scoring table below, operators of government-owned and privately-owned **ground-based infrastructure that support the provision of space-based services** were also considered to be added to the NIS scope, also in consideration of the consistency with the review of the Directive on the identification and designation of European critical infrastructures.<sup>127</sup> Ground-based infrastructure performs essential functions, including control, monitoring, tracking and data collection activities. Space-based services are playing an increasingly important role for the economy and society as a whole and are important for the daily operations of many other critical and important entities. The sector exhibits a very high degree of digital intensity and its operators are highly interconnected with other parts of the economy, making them a likely target for cyber-attacks. Given the large economies of scale that prevail in the provision of space-based services, the sector also exhibits a particularly strong pan-European dimension.

Furthermore additional **subsectors** would also be added for the energy sector, and in particular: district heating, electricity generation, central oil stockholding entities, nominated electricity market operators and electricity market participants providing aggregation, demand response or energy storage services, operators of hydrogen production storage and transmission, as well as EU reference laboratories and entities

---

<sup>127</sup> Council 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, OJ L 345, 23.12.2008, p. 75–82.

conducting research and development activities of medicinal products for the healthcare sector.

As regards **manufacturing**, the subsectors selected were chosen based on the same criteria as those applied to the overall selection of new (sub)sectors and services: i.e. existing Member States' policies covering subsectors beyond the scope of the NIS Directive; stakeholders' views reflected in the results of the OPC and the targeted surveys conducted by the NIS review study; sectorial digital intensity; level of importance for society of sectors, subsectors and services as revealed by a major crisis such as COVID-19; interdependency among sectors. Based on these criteria, the following manufacturing sub-sectors would be covered: food products; beverages; basic pharmaceutical products and pharmaceutical preparations; medical devices and in vitro diagnostic medical devices (as defined in point 1 of Article 2 of Regulation 2017/745 of the European Parliament and of the Council on medical devices, and entities manufacturing in vitro diagnostic medical devices as defined in point 2 of Article 2 of Regulation 2017/746 of the European Parliament and of the Council); medical devices considered as critical during a public health emergency (according to Article 20 of the Commission Proposal for a [Regulation on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices; computer, electronic and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers and semi-trailers; other transport equipment.



<b>Sector/subsector/service</b>	Added by Member States	Consultation results and/or targeted surveys)	Digital intensity	COVID-19 crisis related importance	Level of interdependency of other sectors/subsectors	<b>TOTAL</b>
Electronic communication networks and services <sup>128</sup> (including emergency communication)	2	2	2	2	2	<b>10</b>
Insurance and reinsurance (as part of financial services)	2	n/a	1	0	0	3
Chemicals	2	2	1	0	0	<b>5</b>
Manufacturing	2	1	1	1	1	<b>6</b>
Food supply	2	2	1	2	0	<b>7</b>
Public Administration <sup>129</sup>	2	2	1	1	1	<b>7</b>
Electricity generation	1	2	1	2	1	<b>7</b>
Education (e.g. certain authorities such as those in charge of national exams)	1	n/a	1	0	0	<b>2</b>
Post and other delivery services	1	1	1	2	1	<b>6</b>

<sup>128</sup> This also includes broadcasting services.

<sup>129</sup> This also includes elections (authorities, technology and process), as covered by the consultations, and to the extent they are part of public administration as defined at national and/or regional levels.

Heat production and supply	2	2	1	1	1	1	7
Wastewater	2	2	0	1	0	0	5
Waste management	1	2	0	1	1	1	5
Emergency services	1	2	1	2	0	0	6
Online media	0	n/a	2	2	0	0	4
Data centres & Content Delivery Networks	2	2	2	2	2	2	10
Geolocation services	0	2	2	0	1	1	5
Social networks	0	2	2	1	0	0	5
Trust service providers	0	1	2	0	2	2	5

**EVALUATION  
OF  
DIRECTIVE (EU) 2016/1148 CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF  
SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION  
("NIS DIRECTIVE ")**

**Table of contents**

a)	Introduction .....	84
	Purpose and scope .....	84
b)	Background to the intervention .....	85
	Description of the intervention and its backgrounds .....	85
	The adoption and implementation context .....	86
	Intervention logic of the NIS Directive .....	90
	Baseline and points of comparison.....	91
c)	Implementation / state of Play .....	92
	Description of the current situation .....	92
d)	Method.....	105
	Short description of methodology .....	105
	Deviations from the Roadmap.....	106
	Limitations and robustness of findings .....	107
e)	Analysis and answers to the evaluation questions.....	107
	Relevance .....	107
	Coherence .....	110
	EU Added Value .....	111
	Effectiveness .....	113
	Efficiency .....	115
f)	Conclusions .....	116

## Glossary

<i>Term or acronym</i>	<i>Meaning or definition</i>
CDN	Content delivery network
CSIRTs	Computer Security Incident Response Teams
DNS	Domain Name System
DORA	Digital Operational Resilience Act for the financial sector
DSP	Digital service provider
The ECI Directive	The Directive on the identification and designation of European critical infrastructures
EASA	The European Union Aviation Safety Agency
EECC	European Electronic Communications Code
eIDAS (Regulation)	Regulation on electronic identification and trust services for electronic transactions in the internal market
ENISA	The European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
ICT	Information Communication Technology
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
IXP	Internet Exchange Points
MeliCERTes	Cybersecurity Digital Service Infrastructure Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs
NCA	National Competent Authority
NIS Directive	Directive concerning measures for a high common level of security of network and information systems across the Union
OES	Operator of essential services

PPP	Public Private Partnerships
PSD2	Payment Services Directive 2
SME	Small and medium-sized enterprises
SPOC	Single Point of Contact
TFEU	Treaty on the Functioning of the European Union
TLD	Top-level domain

## a) INTRODUCTION

### **Purpose and scope**

Directive (EU) 2016/1148<sup>130</sup> concerning measures for a high common level of security of network and information systems across the Union (“NIS Directive” or “the Directive”) is the first horizontal internal market instrument aimed at improving the cybersecurity resilience of the European Union. Adopted in July 2016, the NIS Directive has ensured the continuity of essential services allowing the European Union's economy and society to function properly, building cybersecurity capabilities across the EU and mitigating growing threats to network and information systems used to provide essential services in key sectors.

Article 23 of the Directive requires the European Commission to review the functioning of the Directive periodically and to report to the European Parliament and the Council for the first time by 9 May 2021. Meanwhile, the speedy digital transformation of our society has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. The COVID 19 crisis and the resulting sudden growth in demand for internet-based solutions has emphasised even more the need for a state of the art cybersecurity. Therefore, as part of its key policy objective to make “Europe fit for the digital age”, the Commission announced in its Work Programme 2020 that it would advance the review of the Directive to the end of 2020<sup>131</sup>.

The evaluation process started already mid 2019 with the Commission’s “NIS country visits” across all Member States and with a Report from October 2019 assessing the consistency of the approaches in the identification of operators of essential services<sup>132</sup> (“the OES Report”), which was adopted pursuant to Article 23(1) of the Directive. The implementation of the NIS Directive has been the subject of the discussions with the Member States’ competent authorities and ENISA in the NIS Cooperation Group. The present Evaluation Report also takes into account the reports from the Cooperation Group and CSIRTs Network on the experience gained at a strategic and operational level.<sup>133</sup>

The Commission carried out an open public consultation collecting views from all stakeholders. A wide range of stakeholders were consulted as part of the evaluation. These included competent authorities from the Member States, operators from all sectors

---

<sup>130</sup> 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, OJL 194/1, 19.7.2016.

<sup>131</sup> COM (EU) (2020) 37 final, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Commission Work Programme 2020, Brussels, 29.1.2020.

<sup>132</sup> COM (EU) 2019/546 final, Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive [2016/1148/EU](#) on security of network and information systems, Brussels, 28.10.2019.

<sup>133</sup> See Article 23 (2) NIS Directive. According to Articles 11 (4) and 12 (4), the Cooperation Group and the CSIRTs Network have to report on the experiences gained respectively with the strategic and operational cooperation by 9 August 2018 and every year and a half thereafter. Both the Cooperation Group as well as the CSIRTs Network have reported twice on their respective experiences gained (in August 2018 and in January 2020).

under the Directive and Member States, digital service providers, academia and think tanks and the general public. The Commission was supported by an external study<sup>134</sup>, which carried out targeted surveys and interviews and organized dedicated workshops and finally provided input to the evaluation and drafting of the impact assessment.

The review evaluates the functioning of the NIS Directive based on the level of security of network and information systems in the Member States. In accordance with the Better Regulation Guidelines, the evaluation assesses the effectiveness, efficiency, coherence, relevance and EU added value of the NIS Directive taking into account the constantly evolving technological and threat landscape. It pays attention to the impact of the NIS Directive on increasing the levels of cybersecurity across the Union, in particular on the level of national cybersecurity capabilities and the capacity to mitigate growing security threats to network and information systems used to provide essential services in key sectors. The evaluation elaborates on the lessons learned from the implementation of the NIS Directive and identifies persisting and emerging issues affecting the functioning of the Directive. The evaluation also attempts to identify and quantify the direct and indirect regulatory costs and benefits resulting from the implementation of the NIS Directive.

The evaluation focuses on the period starting from the end of the transposition deadline in May 2018 and covers all Member States. Depending on the results from the evaluation of the functioning of the NIS Directive and an impact assessment, the Commission might propose measures aimed at enhancing the level of cybersecurity within the Union.

This staff working document describes the evaluation, how it was carried out, and what it found.

## **b) BACKGROUND TO THE INTERVENTION**

### **Description of the intervention and its backgrounds**

Based on Article 114 of the Treaty on the Functioning of the European Union (TFEU)<sup>135</sup>, the NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU, in order to contribute to the overall functioning of the internal market, by ensuring:

- a) a high level of preparedness of Member States by requiring them to adopt a national strategy on the security of network and information systems and designate: one or more national Computer Security Incident Response Teams (CSIRTs) responsible for risk and incident handling, a single point of contact (SPOC) which shall exercise a liaison function to ensure cross-border cooperation between the Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group, and a competent national NIS authority;
- b) cooperation among all the Member States by establishing the Cooperation Group to support and facilitate strategic cooperation and the exchange of information among

---

<sup>134</sup> An external study carried out by a consortium of Wavestone, ICF and the Centre for European Policy Studies (CEPS), supported the Commission during the evaluation and impact assessment process. The study kicked off in April 2020 and should be finalised by January 2021. The final report of the study was not yet submitted at the time of writing of this report.

<sup>135</sup> Treaty on the Functioning of the European Union, OJ C 326/47, 26.10.2012.

- Member States, and the CSIRTs Network, which promotes swift and effective operational cooperation between national CSIRTs; and
- c) a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure.

Public and private entities identified by the Member States as operators of essential services (OESs) in these sectors are required to undertake a risk assessment and put in place appropriate and proportionate security measures as well as to notify serious incidents to the relevant authorities. Also providers of key digital services (DSPs) such as search engines, cloud computing services and online marketplaces have to comply with the security and notification requirements under the Directive; at the same time, the latter are subject to a so-called ‘light-touch’ regulatory regime which entails, among others, that they are under the jurisdiction of one Member State for the whole EU and are not subjected to ex-ante supervisory measures.

### **The adoption and implementation context**

Cybersecurity resilience is a key priority for the protection of critical infrastructure in the European Union, where network and information systems could be vulnerable due to the fragmented nature of national strategies and capabilities. At a time when the private and public sectors rely increasingly on digital infrastructure for the delivery of essential services, those become major targets of cyberattacks. The companies’ incentives to invest in cybersecurity are insufficient and the benefits of the disclosure of incidents and data breaches – more efficacy and cost savings in security – usually are slower and benefit all firms (including competitors). Ultimately, in an interconnected society, only a collective and coordinated effort between private and public organisations, and national and European players can lead to sufficient levels of cybersecurity resilience.

Against this background, the EU started building the foundations of its current cybersecurity policy. In 2004, the European Network and Information Security Agency (ENISA), was founded. In 2009, the Commission’s Communication was adopted, which focuses on awareness and defines an immediate action plan to strengthen the European cybersecurity resilience<sup>136</sup>. This Communication was followed in 2013 by the joint Communication on a Cybersecurity Strategy to guide the Union’s policy response to cyber threats and risks<sup>137</sup>.

As part of this package, the Commission adopted a Proposal for Directive concerning measures to ensure a high common level of network and information security across the Union<sup>138</sup>. After almost three years of negotiations, a political agreement was reached at the end of 2015, with the understanding that approach to cybersecurity limited to the

---

<sup>136</sup> COM (EU) (2009) 149 final, Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection “Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Brussels, 30.3.2009.

<sup>137</sup> JOIN (EU) (2013) 1 final, Joint Communication to the European Parliament, the Council the European Economic and Social Committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013.

<sup>138</sup> COM (2013) 48 final, SWD (2013) 31 final of 7 February 2013.



national dimension could have put the Digital Single Market at risk<sup>139</sup>. The finally adopted NIS Directive was ground-breaking as it was the first EU legislative act to regulative cybersecurity across sectors. It also complemented the protection of personal data, privacy, the provision of electronic communications services and electronic interactions between businesses, citizens and public authorities offered respectively by the General Data Protection Regulation (GDPR)<sup>140</sup>, the E-Privacy Directive<sup>141</sup>, the Framework Directive on electronic communications networks and services<sup>142</sup> and the eIDAS Regulation<sup>143</sup>.

The NIS Directive has laid the foundations for a European cybersecurity framework and emphasised the need for Member States to secure their own infrastructures in order to function consistently across the European Union. At the same time, the Directive has left large room for discretion to Member States in the implementation of the Directive's objective by requiring a minimum level of harmonisation of the actions to be put in place (Article 3).<sup>144</sup>

To reduce the degree of divergence in the implementation between European countries, a Cooperation Group made up of national representatives, ENISA<sup>145</sup>, and the European Commission, has been tasked to provide strategic direction<sup>146</sup> including guidance on transposition of the Directive (Article 11); and a network of CSIRTs have also been created to ensure that good practice is communicated and exchanged, as well as to support Member States in the implementation of the Directive (Article 12)<sup>147</sup>.

---

<sup>139</sup> Sumroy, R., Donovan, N., (2015), "The NIS Directive: Genesis, Status and Key Aspects", *Slaughter & May*, Briefing June 2015.

<sup>140</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJL 119/1, 4.5.2016.

<sup>141</sup> Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJL 201/37, 31.7.2002.

<sup>142</sup> 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), OJL 108, 24.4.2002, p. 33–50.

<sup>143</sup> 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. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG)

<sup>144</sup> With the exception of security or notification requirements on digital service providers, regarding which the Member States shall not impose any further requirements than those prescribed by the NIS Directive, see Article 3 and Article 16(10) of the NIS Directive.

<sup>145</sup> ENISA has become the European Union Agency for Cybersecurity, with a new permanent mandate, and it has been able to perform new tasks as defined by the EU Cybersecurity Act, which entered into force in June 2019.

<sup>146</sup> See Article 11 of the NIS Directive; Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

<sup>147</sup> Billois, G., (2017), "Cybersecurity and the NIS Directive. A challenge of Consistency for the European Union", Letter from the Wavestone Cybersecurity and Digital Trust Consultant. *Risk Insight*. at: <https://uk.wavestone.com/app/uploads/2017/02/cybersecurity-nis-directive-europe-2.pdf> (last accessed on 21.05.2020).

By establishing a background for cooperation and helping Member States with lower cybersecurity maturity levels to develop their cybersecurity capabilities, the NIS Directive has triggered mind-set change in relation to cybersecurity. Even if cybersecurity, national security and state-sovereignty are still perceived as closely related, the NIS Directive has managed to overcome past concerns regarding sovereign control, helping Member States to experience the benefits of acting together at EU level.

Furthermore, since the adoption of the Cybersecurity Strategy and the last extension of ENISA's mandate in 2013, the overall policy context has changed significantly as the global environment has become more uncertain and less secure. In view of the growing role of ENISA as a reference point for advice and expertise, as a facilitator of cooperation and of capacity-building as well as within the framework of the new Union cybersecurity policy, it became necessary to review ENISA's mandate, to establish its role in the changed cybersecurity ecosystem and to ensure that it contributes effectively to the Union's response to cybersecurity challenges emanating from the radically transformed cyber threat landscape.<sup>148</sup> As a result, the Cybersecurity Act<sup>149</sup> adopted in 2019 granted a permanent mandate to ENISA, more resources and new tasks. The Cybersecurity Act also introduced for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes.

In July 2020, the Commission adopted the EU Security Union Strategy<sup>150</sup>, which acknowledged the increasing interconnection and interdependency between physical and digital infrastructures, and underlined the need for a more coherent approach between specifically the NIS Directive and the European Critical Infrastructure Directive (ECI Directive). The 2019 evaluation of the ECI Directive<sup>151</sup> showed that the landscape related to critical infrastructure protection has changed since the adoption in 2008. To this end, the Commission Work Programme 2020<sup>152</sup> has also planned a proposal for additional measures on critical infrastructure protection until the end of 2020<sup>153</sup>.

The EU Security Union Strategy also underlines the importance of sector-specific initiatives to tackle the specific risks faced by critical infrastructures and to accompany the horizontal frameworks. One such initiative is the Proposal for a Regulation on Digital

---

<sup>148</sup> See Recital 16 of REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

<sup>149</sup> REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

<sup>150</sup> Communication on the EU Security Union Strategy, COM(2020) 605, 24 July 2020 (Strategic priority 'A future-proof security environment').

<sup>151</sup> Council 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. The objective of the Directive is to strengthen the protection of critical infrastructures in the energy and transport sectors.

<sup>152</sup> COM (EU) (2020) 37 final, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Commission Work Programme 2020, Brussels, 29.1.2020.

<sup>153</sup> Security Union Strategy of 24 July 2020, <https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf>; DG HOME, Roadmap regarding new rules regarding the protection of critical infrastructure in the EU, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection>

Operational Resilience for the financial sector (DORA)<sup>154</sup>, which is part of the digital finance package<sup>155</sup>, adopted on 24 September 2020. DORA aims at strengthening the digital operational resilience of the EU financial sector entities, including their ICT security, by streamlining and upgrading existing rules and introducing requirements where gaps exist. DORA would constitute a *lex specialis* to the NIS Directive, at the same time ensuring that details of significant incidents would be passed on from the competent financial authorities to the SPOCs under the NIS Directive and that there will be exchange of information between the financial authorities and the NIS authorities within the framework of the NIS Cooperation Group. In addition, as part of the digital finance package, the Commission put forward a digital finance strategy and a legislative proposal on Crypto Assets aiming to increase the robustness of digital services against cyberattacks<sup>156</sup>.

Other sectorial initiatives are the Network code for the cybersecurity of cross-border electricity flows<sup>157</sup> and the initiative on the protection and cybersecurity of critical energy infrastructure.

Furthermore, in the transport sector, the Union adopted detailed rules for cybersecurity in the aviation security domain<sup>158</sup>. The EU Aviation Safety Agency (EASA) is preparing an opinion to be submitted to the European Commission in order to amend aviation safety legislation with cybersecurity provisions requiring the mandatory introduction of an Information Security Management System.

Last but not least, the Framework Directive<sup>159</sup>, which was amended by the European Electronic Communication Code<sup>160</sup>, also requires Member States to ensure that operators falling under its scope take the necessary risk management measures to secure their networks and to report significant incidents. However, the NIS Directive obligations do not apply as far as the provision of public electronic communication networks or of publicly available electronic communication services are concerned (Article 1 (3) NIS Directive).

---

<sup>154</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 of 24 September 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1>

<sup>155</sup> [https://ec.europa.eu/info/publications/200924-digital-finance-proposals\\_en](https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en)

<sup>156</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. [https://ec.europa.eu/finance/docs/law/200924-crypto-assets-proposal\\_en.pdf](https://ec.europa.eu/finance/docs/law/200924-crypto-assets-proposal_en.pdf)

<sup>157</sup> As empowered by Regulation (EU) 2019/943 on the internal market for electricity. Preparatory work was finalised in September 2019, an informal drafting process is ongoing.

<sup>158</sup> Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2019.246.01.0015.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.246.01.0015.01.ENG)

<sup>159</sup> 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 in 2009, OJ L 108, 24.4.2002, p. 33–50.

<sup>160</sup> See Article 40 of DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code.

## Intervention logic of the NIS Directive

The intervention logic presented in the below chart aims to depict the chain of expected effects associated with the NIS Directive.<sup>161</sup>

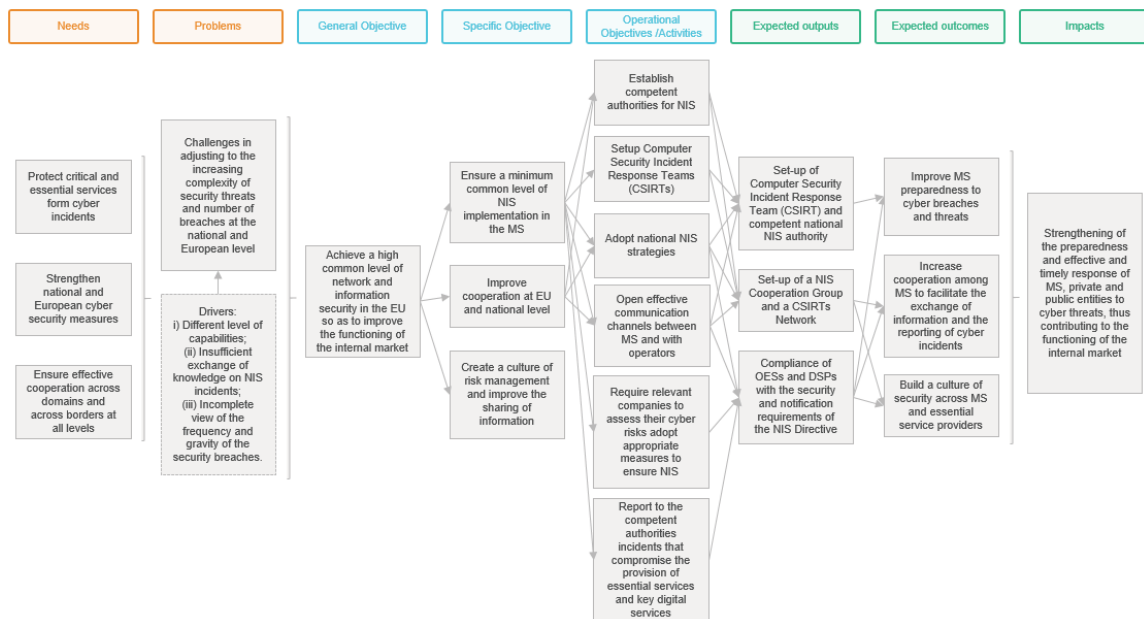


Figure 1: The NIS Directive intervention logic

The above chart helps in visualising the *problem* that the Directive was intended to address when it was first adopted, namely the overall insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal Market.

It looks at the *drivers* behind the problems: the significant disparities in Member States' capabilities and level of preparedness, the insufficient sharing of information on cybersecurity incidents and threats between Member States and key operators and digital service providers and the incomplete view of the frequency and gravity of the security incidents.

Most importantly, it flags the *main objectives* of the Directive. The general objective of guaranteeing a high common level of security on network and information systems in the Union could be translated into *specific objectives* and further *operational objectives*. The specific objectives are (1) to ensure a minimum common level of security of network and information systems implementation in the Member States and thus increase the overall level of preparedness and response, (2) to improve cooperation at Union and at national level with a view to counter cross-border incidents and threats effectively and (3) to create a culture of risk management and sharing of information by OES and DSPs. They should be achieved via the establishment of national competent authorities, CSIRTs, the adoption of national strategies, the creation of links and communication channels

<sup>161</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

between the Member States and with the operators (e.g. via the process of identification), establishing risk management and incident reporting requirements on operators.

These objective should have translated into specific *outputs* leading to *outcomes*, such as improving Member States preparedness to cyber incidents, increased cooperation and information exchange and building a culture of security across Member States and among essential operators and digital service providers. The overall *impact* of the NIS Directive is to strengthen the preparedness of EU Member States and companies and ensure an effective and timely response to cyber threats, thus contributing to the functioning of the Internal Market.

### **Baseline and points of comparison**

The increasing importance of the security of network and information systems for our economies and societies was recognised for the first time by the Commission in 2001, with the Communication ‘Network and Information Security: Proposal for A European Policy Approach’<sup>162</sup> that stressed the increasing importance of network and information systems’ security for our economies and societies. Furthermore, the EU became an observer to the Council of Europe’s Convention on Cybercrime Committee in 2001, and since 2002, legislation related to cybersecurity matters has been adopted<sup>163</sup>. Before the starting of the process that lead to the adoption of the NIS Directive<sup>164</sup>, the only sector where companies were required to take cybersecurity risk management steps under EU law was the electronic communications sector, regulated at the time by the Framework Directive 2002/21/EC on electronic communications networks and services<sup>165</sup> but there was no horizontal instrument aimed at improving the cybersecurity resilience of the Union.

In order to ensure a high and effective level of network and information security in the EU, the European Network and Information Security Agency (ENISA)<sup>166</sup> was established in 2004. The approach adopted at that stage by the European Union in the area of network and information systems has mainly consisted in the adoption of a series of action plans and strategies urging the Member States to increase their cybersecurity capabilities and to cooperate to counter cross-border cybersecurity problems.<sup>167</sup>

---

<sup>162</sup> COM (EU) 2001/0298 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach, Brussels, 6.6.2001.

<sup>163</sup> European Court of Auditors (2019), Challenges to Effective EU Cybersecurity Policy, Briefing Paper, No 02/2019. Available at [https://www.eca.europa.eu/Lists/ECADocuments/BRP\\_CYBERSECURITY/BRP\\_CYBERSECURITY\\_EN.pdf](https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf) (last accessed on 17.06.2020).

<sup>164</sup> COM (EU) (2009) 149 final, Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection ‘Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Brussels, 30.3.2009.

<sup>165</sup> 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), OJL 108/33, 24.4.2002.

<sup>166</sup> The Cybersecurity Act changed ENISA’s name to the European Union Agency for Cybersecurity.

<sup>167</sup> COM (EU) (2013) 48 final, Proposal for a Directive Of The European Parliament And Of The Council concerning measures to ensure a high common level of network and information security across the Union, Brussels, 7.2.2013.

In 2015, before the NIS Directive was adopted, almost one third of the Member States did not have a cybersecurity national strategy. Only a small group of Member States had adopted legislation and policy initiatives to address security of networks and information systems.<sup>168</sup> Many Member States did not have an operational CSIRT to deal with cybersecurity incidents. In 2015, there were no common security and notification requirements on OES and DSPs with the exception of telecommunications companies. In 2015, the majority of the Member States have not done a risk analysis of their assets to determine which national infrastructures were considered to be critical for the functioning of the economy and society<sup>169</sup>.

Without the adoption of the NIS Directive, i.e. under a voluntary approach, the Commission, with the support of ENISA, could have made use of soft law measures such as for example recommendations or guidelines to encourage the Member States to reach a minimum harmonisation of cybersecurity, to set up CSIRTs, and to adopt a national cyber security strategy.

However, doing so, it would have been unlikely that all the Member States would have improved their national capabilities and preparedness. Cross-border cooperation efforts and coordination across all EU Member States to respond to risks and incidents would have taken place only to a very limited extent. It is also less probable that key private players would have managed security risks as effectively as they have done after the introduction of requirements to implement cybersecurity risk management.

Given the interdependency of European networks and systems, with a voluntary cooperation and a voluntary alignment of cybersecurity requirements, the negative impact of cybersecurity incidents and threats on the EU economy and society could have been significant, with the risk of undermining trust in the digital agenda and endangering the Internal Market.<sup>170</sup>

### **c) IMPLEMENTATION / STATE OF PLAY**

#### **Description of the current situation**

##### **Implementation process**

The NIS Directive was adopted in July 2016 and entered into force in August 2016. Member States had until 9 May 2018 to adopt national measures necessary to comply with provisions of the Directive. 17 Member States had not communicated transposition by this deadline. The Commission started infringement procedures by sending letters of formal notice to these Member States in July 2018. By September 2019, all Member States had communicated full transposition.

---

<sup>168</sup> BSA, the Software Alliance (2015), EU Cyber security Dashboard: A Path to a Secure European Cyberspace. Available at: [http://cybersecurity.bsa.org/assets/PDFs/study\\_eucybersecurity\\_en.pdf](http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf).

<sup>169</sup> COM (EU) 2019/546 final, Report From The Commission To The European Parliament And The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, Brussels, 28.10.2019.

<sup>170</sup> SWD (EU) 2013/032 final, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, Strasbourg, 7.2.2013.

In the context of the implementation of the NIS Directive, Member States were required to define essential services and identify operators of essential services in their territories based on criteria set up in the Directive. Article 5(7) of the Directive requires Member States to report to the Commission on the results of this identification. In accordance with Article 23(1), the Commission was tasked to draft a report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services (“the OES Report”) and to submit it to the European Parliament and the Council by 9 May 2019. The OES Report was based on an assessment conducted between November 2018 and September 2019. In view of these delays in the identification process and the lacking information from a number of Member States, the report was only published on 28 October 2019.

In July 2019, the Commission sent letters of formal notice to 6 Member States for failure to comply with their obligations under Article 5(7). At the time of drafting of the present Evaluation Report, 3 of the started infringement procedures are still ongoing.

In addition to the OES Report, in view of its obligation under Article 23(2) to report on the functioning of the Directive, the Commission has been carrying out “NIS country visits” across the Member States from June 2019 to July 2020<sup>171</sup>. During these country visits aiming to assess on the spot the level of transposition and implementation of the NIS Directive and to receive feedback both from the industry and the relevant authorities about the effects and challenges brought by the Directive, the Commission interviewed various stakeholders – OES from different sectors, DSPs, national competent authorities, SPOCs and CSIRTs.

### **Implementing and transposing measures**

#### *National capabilities – national strategies, setting up of national competent authorities, SPOC and CSIRT*

The NIS Directive requires Member States to adopt a *national cybersecurity strategy* containing at least<sup>172</sup> the seven elements listed in Article 7(1) and to communicate this to the Commission. In 2015, only 19 out of the then 28 Member States had national strategies in place, 8 Member States did not have any strategy and one Member State was in the process of drafting a national strategy<sup>173</sup>. With the implementation of the Directive, all Member States have developed specific national legislation to regulate several aspects of cybersecurity and to put in place concrete initiatives in this direction by assigning the role to each body. Therefore, the adoption of the national strategies gave impetus to the implementation of a series of concrete policy actions such as the definition of a risk-assessment plan, a governance framework to achieve the objectives of the national strategy and the identification of measure related to cybersecurity capacity building such as preparedness, response and recovery<sup>174</sup>. This legal provision helped the Member States

---

<sup>171</sup> Due to the COVID-19 crisis, 12 out of the 27 NIS country visits were carried out in a virtual format.

<sup>172</sup> Communication from the Commission to the European Parliament and the Council, “Making the most of NIS”, COM (2017) 476 final 2 4 October 2017, p. 6.

<sup>173</sup> Business Software Alliance (2015), EU Cyber security Dashboard: A Path to a Secure European Cyberspace.

<sup>174</sup> Bird & Bird (2020), Developments on NIS Directive in EU Member States and ENISA- (2020) National Cyber Security Strategies- Interactive Map. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

with less capacity to make a substantial step forward in cybersecurity preparedness, ensuring a high level of security in their territory.<sup>175</sup>

The NIS Directive also requires Member States to designate one or more *competent authorities* to implement the provisions of the Directive for the key sectors and digital services under its scope. In addition, Member States have to put in place a single point of contact (SPOC) for cross-border cooperation and one or more *computer security incident response teams (CSIRTs)* for incident handling.

All Member State now have designated NCAs, a SPOC and CSIRT(s)<sup>176</sup>. However, some Member States (14) opted for a centralised approach designating a single national authority for DSPs, OESs, and as a SPOC, while others (14 Member States) have decided to designate several sectoral authorities to coordinate their actions.<sup>177</sup>

Before the NIS Directive came into force not all the Member States had a CSIRT in place. Nowadays, all Member States have at least one or even more (sectorial) CSIRTs<sup>178</sup> and have to ensure that these CSIRTs have adequate resources to effectively carry out their tasks under the Directive. More than 90 percent of all national CSIRTs or government teams with national scope reached the basic maturity level, averagely being close to reaching the intermediate maturity level<sup>179</sup>.

Some Member States have fostered the development of fora where companies can exchange information about cybersecurity. This includes inter alia public private partnerships (PPPs) or sectorial Information Sharing and Analysis Centres (ISACs). In 2015 only five Member States had established formal PPPs for cybersecurity and in 2020 these partnerships are still lacking in eleven Member States. The below chart sums up the state of play of national capabilities among the 27 Member States and the UK:

---

<sup>175</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>176</sup> Bird & Bird (2020), Developments on NIS Directive in EU Member States and ENISA- (2020) National Cyber Security Strategies- Interactive Map. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

<sup>177</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>178</sup> ENISA (2019), Study on CSIRT landscape and IR capabilities in Europe 2025. Available at: <https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025> (last accessed on 16.05.2020).

<sup>179</sup> TI Accreditation was used as baseline for the Basic Maturity Level <https://www.trusted-introducer.org/processes/accreditation.html>



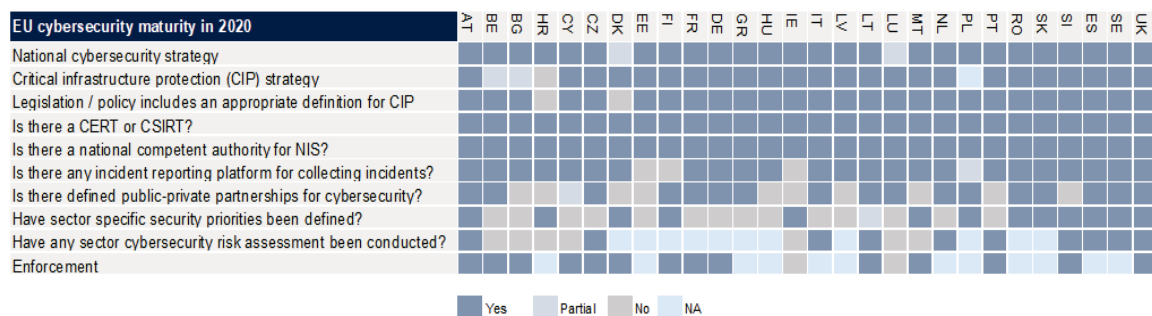


Figure 2 EU cybersecurity maturity in 2020<sup>180</sup>

Overall, during the evaluation, a lack of adequate financial resources and staffing emerged as one of the most relevant challenges that national competent authorities pointed out in the implementation of the NIS Directive. This is linked to the difficulty for national administrations to offer competitive salaries for highly skilled employees. In some Member States, no additional staff has been recruited. Instead, the available staff members have been tasked with the implementation of the NIS Directive in addition to their usual responsibilities.

### OES identification

The NIS Directive does not determine which companies will be included as OES under its scope. Instead, Article 5(2) sets out criteria that Member States will need to apply in order to carry out an identification process, which will ultimately determine which companies belonging to the type of entities under Annex II will be considered as OES and be subject to the NIS Directive. Annex II lists seven core economic sectors and their subsectors considered as essential for the effective functioning of the internal market: energy (electricity, oil, gas), transport (air, rail, water and road), banking, financial market infrastructures, health sector (including hospitals and private clinics), drinking water supply and distribution, and digital infrastructure (IXPs, DNS service providers and TLD name registers). These sectors have been chosen based on their potential vulnerabilities to threats and attacks, due to their high dependence on network and information systems and due to their essential role for the functioning of the internal market in the Union.

Member States have been given large room of discretion in selecting the relevant entities in order to account for national specificities.<sup>181</sup> In the absence of detailed guidance on how to identify OESs, Member States have developed a variety of *methodologies*,<sup>182</sup> also with regard to the definition of essential services and the setting of thresholds.<sup>183</sup> For example there are Member States, in which public authorities conduct the identification process (top-down identification) and Member States, in which operators were required

<sup>180</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report; based on BSA (2015), Bird & Bird (2020), ENISA (2020).

<sup>181</sup> COM (EU) 2019/546 final, Report From The Commission To The European Parliament And The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems (OES Report), 28.10.2019, Section. 1.1.3.

<sup>182</sup> OES Report, Section. 2.1.

<sup>183</sup> OES Report, Sections 2.1 and 2.3.

to verify themselves whether they meet the national criteria (self-identification).<sup>184</sup> One of the elements influencing national methodologies was the pre-existence of a framework on critical infrastructures or other national provisions on “vital operators”. In such cases, Member States used their prior experience as a point of reference and incorporated specificities related to the NIS Directive into existing methodologies. Differences in national methodologies fall in the following main categories: essential services, use of thresholds and their levels, degree of centralisation, authorities in charge of identification and assessment of network and information systems dependence.<sup>185</sup>

As regards the *definition of essential services*, Member States apply different levels of granularity: some provide a list of detailed services they consider essential, whereas other Member States indicate only general types of services leaving room for interpretation.<sup>186</sup> As concluded by the OES Report, this leads to consistency gaps, which renders it difficult to compare the lists of essential services and, more importantly may lead to fragmentation, if operators in one Member State are exposed to additional regulation while others providing similar services in another Member State are excluded.<sup>187</sup> The *numbers of services* identified also varies greatly between Member States. With an average of 35 services per Member State, the number of identified services ranges from 12 to 87, as shown in Figure 3 below.

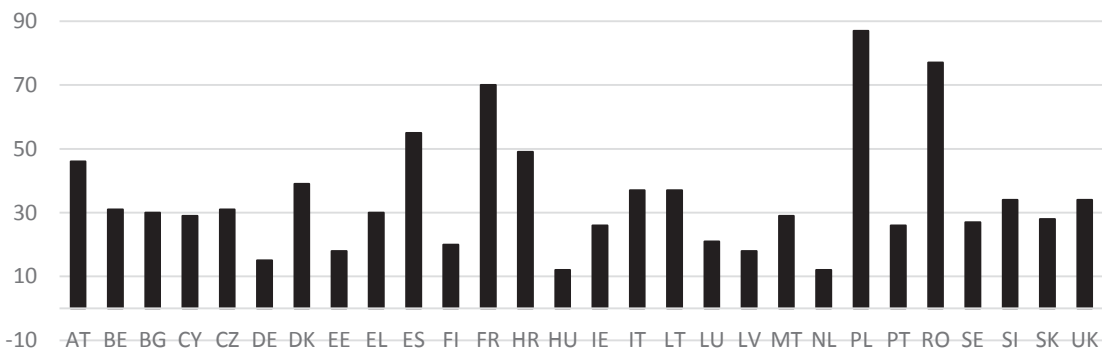


Figure 3: Overall number of essential services identified by Member States

Most Member States apply thresholds to identify OESs, which can be sector-specific or cross-sectoral and vary from Member State to Member State.<sup>188</sup> They may rely on a single quantitative factor, a larger set of quantitative factors or a combination of quantitative and qualitative factors.<sup>189</sup> The various approaches taken by Member States have ultimately led to very different result also in the number of identified operators in the sectors and subsectors.<sup>190</sup>

<sup>184</sup> OES Report, Section 2.1.

<sup>185</sup> OES Report, Section 2.1.

<sup>186</sup> OES Report, Section 2.2 taking the example of approaches chosen by Member States in the identification of essential services in the electricity subsector, where Estonia takes the least granular approach with ‘electricity supply’, whereas Bulgaria with the most granular approach enlist the ‘distribution of electricity’, ‘ensuring the functioning and maintenance of a distribution system for electrical energy’, ‘transmission of electricity’, ‘operation, maintenance and development of an electricity transmission system’, ‘electricity production’ and ‘electricity market’.

<sup>187</sup> OES Report, Sec. 2.2.

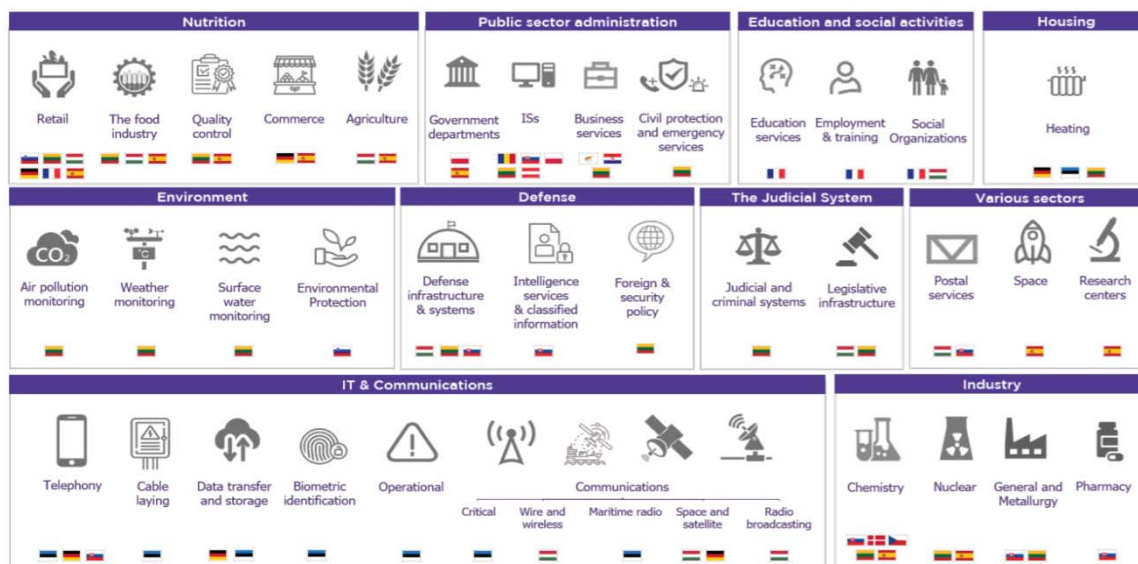
<sup>188</sup> OES Report, Section 2.3.

<sup>189</sup> OES Report, Section 2.3.

<sup>190</sup> OES Report, Section 2.4.

The minimum harmonisation approach of the NIS Directive allows Member States to consider in the implementation also services that are not provided by entities in the sectors included in Annex II. The OES Report reveals that to reinforce cybersecurity in other sectors that Member States consider nationally sensitive, 11 out of 28 Member States have identified essential services in additional sectors. This highlights that there might be other sectors that are critical for society and the economy and also potentially vulnerable to cyber-incidents that should be considered by the Directive<sup>191</sup> (See Figure 4 below).

Figure 4: Additional sectors and subsectors identified by Member State<sup>192</sup>



As regards the organization of competent authorities at a national level, there are different degrees of centralisation when it comes to the authorities responsible for defining essential services and identifying operators with some Member States nominating a single authority in some others more than one. In some cases, operators were identified by a competent authority or a CSIRTs while in other cases by primary legislation or even through self-assessment and self-identification.<sup>193</sup>

Another issue related to the identification of OES is the cross-border procedure under Article 5(4) requiring Member States to engage in consultation with each other before reaching a final identification decision. The Cooperation Group has issued a reference document in July 2018 in order to help Member States conduct proper cross-border consultations.<sup>194</sup> However, it appears that only very few national authorities have made use of this tool at all or at least in a comprehensive and consistent manner. Among the possible explanations could be the time that it took Member States to carry out the identification, the lack of secure channel for communication, the lack of common

<sup>191</sup> OES Report, Section 2.5.

<sup>192</sup> The NIS Directive, An Overview of Transposition In Europe For Operators Of Essential Services (OESs), June 2020, based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report..

<sup>193</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>194</sup> *Identification of Operators of Essential Services – Reference document on modalities of the consultation process in cases with cross-border impact*, Cooperation Group Publication 07/2018.

understanding of the cross-border consultation process or the large number of cross-border operators active across several Member States<sup>195</sup>.

Finally, there appears to be a level of inconsistency with regard to the application of the *lex specialis* principle of Article 1(7). While most Member States identified OES in the banking and financial markets sector, a few Member States have not done so based on the argument that operators are providing services covered by *lex specialis*.<sup>196</sup> Similarly, some Member States appear to have identified OES that should be regulated under the European Electronic Communications Code (EECC) and thus falling under the provision of Article 1(3).<sup>197</sup> Others have decided to completely exclude providers of electronic communications networks or services, which also supply digital infrastructure services from the scope of the NIS Directive and only apply the EECC.

#### *Digital service providers*

The notion of “digital service” is defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services” which is of the type listed in Annex III of the Directive (Article 4(5)). Contrary to OES, the list of digital services in Annex III is applied in a homogeneous way in the Member States by all providers under the scope of the Directive<sup>198</sup> (as opposed to being identified per each Member State as is the case for OES). The list is limited to three types of digital services as per Annex III: cloud computing services, online marketplace and online search engines, selected due to their significant criticality as assessed by the time of adoption in 2016.

While Member States are allowed to impose stricter security and notification requirements for OESs than those enshrined in the Directive, they are prohibited to do so for DSPs according to Article 3 and 16(10) of the NIS Directive (the so-called principle of “maximum harmonisation”). Moreover, national competent authorities can only supervise DSPs "ex-post", when an authority is provided with evidence that a company does not fulfil its obligations.

Because of their cross-border nature, DSPs are also subject to one single jurisdiction within the EU based on the Member State of their main establishment. Pursuant to Article 18 of the NIS Directive, a DSP shall be deemed to be under the jurisdiction of the Member State, in which it has its main establishment. It further specifies that the main establishment is where a company’s head office is located. However, the Directive does not provide a precise definition of what constitutes a main establishment or a head office. Competent authorities usually refer to the commercial register to determine the establishment of an entity. However, the information in the national commercial registers is often limited to a particular Member State. Especially in the case of DSPs, which mostly operate across borders and/or have several establishments in the Union, such registers do not contain sufficient information about parent and sister companies throughout the Union to determine the location of the company’s main establishment in the Union.

---

<sup>195</sup> OES Report, Section 2.6.

<sup>196</sup> OES Report, Section 2.7.

<sup>197</sup> OES Report, Section 2.7.

<sup>198</sup> Recital 57 of the NIS Directive.

When DSPs offering services in the Union have no establishment in any Member State, they are required to designate a representative in one of the Member States where the services are offered (Article 18 (2) of the NIS Directive). However, the provisions of the Directive do not require DSPs to inform the competent authority of the very Member State in which they have designated their representative. Therefore, Member States have limited knowledge regarding their own competence for specific DSPs.

Due to the reactive ex-post supervisory approach to DSPs<sup>199</sup>, competent authorities should only take action when provided with evidence that a DSP is not complying with the requirements of the Directive. Thus, there is no general obligation on the competent authority to supervise DSPs. As a result, national competent authorities are cautious in being proactive and contacting the DSPs in order to establish the precise country of jurisdiction. Moreover, while implementing the Directive, in view of often limited resources, national competent authorities tend to prioritize the identification of OES to an effort to understand which DSPs fall under their jurisdiction. This limited overview of competent authorities of the DSPs under their jurisdiction has been regarded as a major obstacle in the enforcement of the obligations towards DSPs.

All these elements of the so-called “light-touch” regulatory approach applied towards DSPs have been motivated primarily by the perception at the time of the adoption of the NIS Directive that cybersecurity incidents in DSPs presented a lower degree of risk to society and the internal market in comparison to OES. However, it can be observed that in the past years, and particularly since the COVID 19 crisis, the digital services are becoming vitally important for the society and the economy. Especially cloud services providers are providing more often services that may be considered critical for the operation of OES services but also serve as infrastructure to many other online services that citizens and the market rely on.

### *Security measures*

Article 14(1) imposes on Member States to ensure that OES, having regard to the state of the art, take appropriate and proportionate technical measures to manage the risk posed to the security of the network and information systems, which the organisations use in the provision of their services.

Member States have opted for very different approaches when designing their national law on security requirements for OES. For example, some countries such as Estonia, France and Romania have decided to include these security measures directly in their legislative texts (laws, decrees, orders or equivalent), whereas in Belgium there is a presumption that OES fulfil the requirements if they comply with, or even obtain, ISO/IEC 27001 certification. This certification specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. For some other Member States, which did not chose to specify the security measures in their laws or use a certification framework, national competent authorities published implementation guidance materials (e.g. Italy)<sup>200</sup>. The consequence is that security requirements show a

<sup>199</sup> See Article 17(1) and Recital 60 of the NIS Directive.

<sup>200</sup> Van Tieghem (2020), ‘The NIS Directive, An Overview of Transposition In Europe For Operators Of Essential Services (OESs)’, Risk Insight. Available at: <https://lu.wavestone.com/en/insight/nis-directive-transposition-operators-essential-services/>; Based on the interim findings of the NIS review

great variation across Member States from granular approaches setting a minimum length for passwords in the absence of two-factor authentication to more general requirements. Usually, they are set by secondary legislation and in some cases are sector-specific while in others follow general rules based on risk analysis and management. This variation in approaches and the diversity in types of measures could lead to an uneven level of preparedness to cybersecurity incidents across EU Member States. Additionally, this makes it complex for multinational companies to comply with the security measures across the EU.<sup>201</sup>

As regards DSPs, Article 16(1) requires Member States to ensure that DSPs identify and take appropriate and proportionate measures to manage the risks posed to the security of the network and information systems which the DSPs use for the provision of their services taking account of the state of the art and a number of elements prescribed by the Directive (the security of systems and facilities; incident handling; business continuity management; monitoring, auditing and testing; and compliance with international standards). These elements are further elaborated in the Commission Implementing Regulation (EU) 2018/151.<sup>202</sup> With regard to security requirements to DSPs, the Directive precludes Member States from imposing any further requirements, i.e. it provides for maximum harmonisation (Article 3 and Article 1(6) of the NIS Directive).

#### *Incident reporting*

Articles 14(3) and 16(3) require OES and DSPs respectively to notify without undue delay the competent authority or CSIRT of any incidents with a significant impact on the continuity of the essential service provided.

With regard to OES, the parameters for a substantial incident are listed in Article 14(4)<sup>203</sup>. The parameters concerning incidents with DSPs are mentioned in Article 16(4)<sup>204</sup> and further specified in the Commission Implementing Regulation EU 2018/151<sup>205</sup>.

---

study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>201</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>202</sup> Article 2 of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

<sup>203</sup> These parameters according to Article 14(3) are the number of users affected by the disruption of the essential service, the duration of the incident and the geographical spread with regard to the area affected by the incident.

<sup>204</sup> The parameters according to Article 16(3) are the number of users, the duration of the incident, the geographical spread, the extent of the disruption of the functioning of the service, the extent of the impact on economic and societal activities.

<sup>205</sup> Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

When it comes to incident notification, the differences across Member States increase even more due to the different values and roles played by the two variables characterising the incident reporting requirements: thresholds and modalities of reporting.

As far as *thresholds* are concerned, in some Member States they do not exist at all and in others they are extremely detailed and/or vary by sectors. The multitude of sectoral approaches reflect the variety of OES and corresponding business models but could provide an obstacle to a common regulatory approach in the EU and to the activity of cross-border operators.

Overall, hardly any incident in the past two years has attained one of the established thresholds and therefore very few incidents are being reported to the national competent authorities<sup>206</sup>. The NIS Cooperation Group recognises that a simple parameter to define the threshold imposed by the Directive, such as ‘number of users’ can mean different things to different types of providers, from simple clients of an electricity provider to potential patients of a hospital<sup>207</sup>. There is also a broad consensus that the thresholds are set too high to trigger the notification under the NIS Directive regime.<sup>208</sup> In few Member States voluntary reporting is envisaged and encouraged through, for instance, the reporting of near-misses<sup>209</sup>.

In terms of the *modalities* of the incident reporting, Member States have opted for different approaches such as the use of online platforms and portals, hotlines or email notifications.<sup>210</sup> The delay for reporting varies across the Member States from “without undue delay” or “immediately” to 24 hours and for the first written or follow-up report from 5 days to 4 weeks. OES and DSPs need to report the incidents to different authorities in the various Member States – for example to the central or sectorial CSIRTs, or national centralised or sectorial competent authorities. In many cases, companies need to report the same incident to several competent authorities within one Member State via several different templates on the basis of overlapping legal requirements.<sup>211</sup> This has been a serious point of concern for both national authorities and operators.

### *Supervision and enforcement*

Article 15 requires Member States to provide competent authorities with the necessary powers and means to supervise operators of essential services. It also lays down the main elements of the ex-ante supervision process operators of essential services are subject to. This process includes the requesting of information and documentation from the entities in question, the gathering of evidence of effective implementation of security policies and the issuing of binding instructions to operators to remedy deficiencies.

---

<sup>206</sup> According to the feedback from the national competent authorities during the NIS country visits.

<sup>207</sup> NIS Cooperation Group (2018), Reference Document on Incident Notification for Operators of Essential Services, CG Publication 02/2018. Available at [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53644](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644), p. 24.

<sup>208</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>209</sup> Such Member States are e.g. in Austria, Lithuania, Slovakia.

<sup>210</sup> For a full picture of the incident reporting modalities across all Member States, see final NIS review study report due by December 2020/January 2021, not yet submitted at the time of the writing of this report

<sup>211</sup> The NIS incident reporting obligations might come in some cases in addition to similar reporting obligations, such as e.g. under GDPR, PSD2, eIDAS.

During the NIS country visits, the Commission has observed that many Member States do not have formal requirements for operators of essential services to submit documentation of their security policies. In even fewer cases, competent authorities are systematically checking whether companies are complying with the NIS rules. In most Member States, national authorities tend to prioritize and promote a collaboration approach focused on cybersecurity awareness instead of audits.<sup>212</sup> Among the companies that the Commission interviewed during the NIS country visits, most companies that have undergone an audit, have launched the procedure by themselves and have done so for reasons not directly linked to the Directive.

When it comes to the supervision of DSPs, Article 17 requires Member States to ensure that competent authorities take ex-post supervisory measures once provided with evidence that a digital service provider does not meet the security requirements or has not notified of a reportable incident<sup>213</sup>. In addition, competent authorities do not have a full picture of the digital service providers falling under their jurisdiction (as explained in the section on *Digital service providers* above). Even though some of the Member States (such as e.g. Ireland or the Netherlands) are aware of the most relevant digital service providers within their jurisdiction, the lack of official ex ante information exchange between DSPs and competent authorities significantly impedes any effective supervision of these service providers.

In terms of *organisational structures*, apart from the constant role that CSIRTs play in all Member State to receive incident notifications and provide assistance when needed, Member States have opted for many different supervisory approaches. Some Member States have a unique national agency to be the competent authority for supervision and enforcement (France, Germany) while others have decided to have sectoral authorities (Spain, Italy, United-Kingdom) or both (Belgium). According to the national legislative transposition, the compliance audits are led by the competent authorities in some countries (Italy, Spain, France) which can decide to delegate it to a qualified third party (Germany, UK). In some others, the OES has the opportunity to directly select the auditor firm, as long as it is qualified by the competent authorities (Belgium, France).<sup>214</sup>

While Article 21 requires Member States to lay down penalties that are “effective, proportionate and dissuasive”, the Directive does not provide any guidance to Member States as to what is considered as effective and dissuasive. As a result, the level of maximum penalties varies greatly between the Member States, ranging from around 1.400 EUR to 5.000.000 EUR or certain percentages of the global annual turnover of undertakings, ranging from 0.5% to 5%. Some Member States have only sector-specific rules, with no specified levels of maximum penalties. The maximum penalties laid down in the national regulations transposing the Directive in most Member States are lower than the average penalty of around 100.000 EUR.<sup>215</sup> Finally, competent authorities have so far been reluctant to actually apply penalties. As a matter of fact, not a single case of a

---

<sup>212</sup> Based on feedback from national competent authorities received during the NIS country visits.

<sup>213</sup> Article 17, Recital 60 of the NIS Directive.

<sup>214</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>215</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.



penalty having been applied to a public or private entity has been brought to the attention of the European Commission at the time of writing of this report.

### *EU Cooperation – Cooperation Group, CSIRTs Network*

The EU Cooperation under the NIS Directive takes place at a strategic level within the NIS Cooperation Group and at an operation level, within the CSIRTs Network.

*The Cooperation Group*<sup>216</sup> is the guiding body in the implementation of the NIS Directive, which aims to facilitate strategic cooperation between Member States and sharing of information, experience and best practice relating to the security of network and information systems. The Group is composed of representatives of the Member States, ENISA and the Commission that also provides the secretariat.

According to Article 11, the Cooperation Group has among others, the following specific tasks: providing strategic guidance to the CSIRTs Network; exchanging best practice on information sharing on incidents, incident notification processes and risks; assisting Member States in building cybersecurity capacity, discussing capabilities and preparedness of Member States and of national cybersecurity strategies and CSIRTs; exchange of information and best practices on awareness-raising, training, research and development of network and information systems, exchanging best practices about the identification of operators of essential services by the Member States and in relation to cross-border dependencies.

The Cooperation Group, meets on a regular basis and is chaired by the respective Member State holding the Presidency of the Council of the EU<sup>217</sup>. The Cooperation Group carries out its tasks on the basis of biennial work programmes. The first Work Programme laid the ground towards shaping the working methods of the Group, building trust between Member States and coming up with the most urgent deliverables. In February 2020, the Cooperation Group adopted its Second Biennial Work Programme (2020-2022). Meanwhile, the Cooperation Group has established itself as a key forum and point of reference for policy discussion on cybersecurity within the EU. Besides the plenary sessions of the Cooperation Group, Member States representatives meet in 12 work streams, where they discuss specific topics such as the identification of OES, security requirements, incident reporting, cross-border dependencies, digital service providers and capacity building. Moreover, for three of the sectors under Annex II of the NIS Directive there are already dedicated work streams – energy, digital infrastructure and health. The Cooperation Group has provided the forum for discussing additional issues of relevance such as elections security and large-scale cyber incidents and crises (Blueprint)<sup>218</sup>. The NIS Cooperation Group provided also the forum for a dedicated working group on the cybersecurity of 5G networks, bringing together competent authorities in order to support and facilitate cooperation. It produced a joint EU risk

---

<sup>216</sup> See NIS Cooperation Group website <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

<sup>217</sup> See Article 2 of COMMISSION IMPLEMENTING DECISION (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0179&from=EN>

<sup>218</sup> COMMISSION RECOMMENDATION of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.

assessment, a toolbox of mitigating measures as well as a progress report on the 5G toolbox implementation.

Among the key outputs of the NIS Cooperation Group are non-binding guidelines to the EU Member States to allow effective and coherent implementation of the NIS Directive across the EU and to address wider cybersecurity policy issues. Since its establishment, the Group has published eight working documents<sup>219</sup> and it is in the process of reviewing and updating some of them. The Cooperation Group has had a crucial role in bringing national authorities closer and creating trust in matters, some of which have been considered close to national security.

*The CSIRTs Network* established by Article 12 is another form of EU cooperation. The CSIRTs Network's aim is to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation. The CSIRTs Network is composed of EU Member States' appointed CSIRTs and CERT-EU. ENISA is tasked to actively support the CSIRTs Network, provide the secretariat and support incident coordination upon request. The European Commission participates in the network as an observer.

The main tasks of the CSIRTs Network are to exchange information on services, operations and cooperation capabilities, share incident information, identify a coordinated response to an incident, provide support to Member States in addressing cross-border incidents, discuss other forms of cooperation linked to early warnings, discussing preparedness and capabilities of Member States and issuing guidelines. The CSIRTs Network has to report to and request guidance from the Cooperation Group.

The rules for the functioning of the CSIRTs Network are defined in its terms of reference. The activity encompasses three meetings per year and the everyday operational cooperation happens mostly using online tools. The activity of the CSIRTs Network is structured in various working groups (such as CyberWeather, Maturity, Standard Operational Procedures and Tools), as well as the participation to cybersecurity exercises organised every year. In line with the Blueprint Recommendation, the CSIRTs Network set out modalities for cooperation and exchange of information in Standard Operating Procedures. These envisage different levels of intensity of cooperation, based on the threats level across the EU, and facilitate a coordinated response to incidents.

The need to get over the different levels of maturity among the national CSIRTs by improving the operational cooperation and facilitating the sharing of information between the EU Member States' CSIRTs and across the EU, has been the focus of the MeliCERTes project developed with the financial support of the EU<sup>220</sup>. Its primary purpose was to facilitate cross-border cooperation encompassing data exchange between two or more CSIRTs based on the concept of trust circles i.e. ad hoc groups of CSIRTs which mutually agree on co-operation based on the concept of trust. MeliCERTes became operational in January 2019 and has been refinanced to advance the facility

---

<sup>219</sup> Available here: <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

<sup>220</sup> Public tender on Connecting Europe facilities — cybersecurity digital service infrastructure — SMART 2015/1089SMART 2015/1089.

MeliCERTes (to develop MeliCERTes II) in accordance with the evolving needs of the CSIRTs in the EU<sup>221</sup>.

The improvement in the cooperation methods by the CSIRTs Network has been shown in times of crisis, such as COVID-19. The CSIRTs Network had two meetings per week at the beginning of the crisis and produced nine reports on different issues and coped overall very well with the new crisis situation offering advice to Member States and improving confidence and trust among its members<sup>222</sup>.

As regards the cooperation between the CSIRTs Network and the Cooperation Group, although Article 11(3)(a) prescribes a role of strategic guidance to the CSIRTs Network for the Cooperation Group, the collaboration between these two fora has been limited to reports by the CSIRTs Network to the Cooperation Group due every year and a half, and to an annual joint session organised back to back with one of the Cooperation Group plenary meetings.

According to ENISA, the creation of the CSIRTs Network, had a very positive impact in clarifying actors' role and responsibilities within the incident response process, improving its overall governance. However, the NIS Directive had an unequal effect from one country to another due to the different pre-existing maturity of Member States with regards to incident response<sup>223</sup>.

#### **d) METHOD**

##### **Short description of methodology**

The present evaluation aims to analyse the implementation and application of the Directive in each Member State according to a number of specific criteria set out in the Commission's Better Regulation Guidelines (relevance, coherence, effectiveness, efficiency, EU added value and sustainability). The evaluation covered all 27 Member States and the UK<sup>224</sup> and their implementation of the Directive since the deadline for its transposition in May 2018.

The consultation activities aimed at collecting the views of Member States' competent authorities, Union bodies dealing with cybersecurity, operators of essential services, digital services providers, companies in other vulnerable sectors outside the scope of the current NIS Directive, trade associations, researchers and academia, cybersecurity industry professionals, consumer organisations and citizens. During the 27 NIS country

---

<sup>221</sup> See MeliCERTSes <https://ec.europa.eu/digital-single-market/en/news/call-tender-advance-melicertes-facility-used-csirts-eu-cooperate-and-exchange-information>. The existing MeliCERTes version is using open source tools developed and maintained by CSIRTs. It allows for the use of any key functions undertaken by the CSIRTs, such as incident management, threat intelligence (encompassing event management, vulnerability management and threat management), secure communications and artefact analysis.

<sup>222</sup> Contractor's interviews with members of the CSIRTs Network. Reference is made especially to the cyber-attacks on hospitals in the beginning of the COVID-19 crisis. Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>223</sup> ENISA (2019), EU MS Incident Response Development Status Report. <https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report>.

<sup>224</sup> No country visit to the UK took place. The evaluation of the impact of the NIS Directive on the UK was mainly based on desk research.

visits, the Commission interviewed the 117 SPOCs, CSIRTs and national competent authorities, 136 OES and 18 DSPs.

In addition to the NIS country visits, which were carried out from June 2019 until July 2020, and the OES Report, the Commission published the NIS Directive review roadmap on 25 June 2020, which was open for feedback until 13 August 2020 and received 42 contributions. From 7 July until 2 October, the Commission held an open public consultation on the NIS Directive review with the general public.

The Commission received 209 stakeholders' replies via the official EU Survey channel. Beside the regular discussion on the implementation of the NIS Directive in the framework of the Cooperation Group and its work streams, the NIS review was discussed at 3 Cooperation Group plenary meetings at the time of writing of the present Report. In addition, the Commission received written contributions from ENISA and from 16 Member States authorities.

Assisted by the external contractor (a consortium of ICF, Wavestone and CEPS), the Commission also collected evidence via desk research, targeted surveys to the different stakeholder groups, 16 expert interviews, 4 workshops with experts and with representatives of national authorities of Member States and businesses in the relevant sectors under scrutiny, as well as other stakeholders. 46 national competent authorities from 24 Member States, 49 OES and 9 DSPs replied to the targeted surveys.

A more detailed presentation of the consultation process is described in the Summary report of the Open Public Consultation (see Annex 2 to the Impact Assessment Report).

### **Deviations from the Roadmap**

The inception impact assessment/roadmap for this initiative, which was published in June 2020 indicated that three regional workshops would be organised gathering Member States, representatives of competent authorities, operators and cybersecurity experts in the third quarter of 2020. However, due to the persisting measures to attenuate the impact of the COVID 19 crisis, these workshops were carried out in a virtual format as webinars. This allowed for a broader than regional participation in each of the workshops. The first workshop took place in June 2020 and drew the attention to the NIS Directive review process and its timing. The attendance was between 80 and over 100 participants respectively for the two sessions, the most active of them coming from national competent authorities.

During the second workshop in July 2020 (attended by over 90 participants), the focus was largely on the shortcomings of the current NIS Directive and improvement ideas. This workshop was well attended also by operators and digital service providers, which actively represented the views of the private sector.

Two Closing Workshops took place on 12 October (for competent authorities, gathering over 65 participants), and 13 October 2020 (for the private sector, gathering over 60 participants). These workshops aimed to engage in a reflection on potential policy options to further enhance the level of protection of network and information systems across Europe and their respective economic, environmental and social impacts accounting for current and future technological developments.

## **Limitations and robustness of findings**

Despite the extensive consultation activities with stakeholders and the open public consultation, there are a number of issues that have affected the robustness of the findings. Such are:

A lack of available evidence, including historical data, and low quality of information in some cases prevented a quantitative analysis of the changes introduced by the NIS Directive. For example, only few stakeholders provided quantitative data on costs and benefits of implementing the NIS Directive, and this made it difficult to quantify and monetise such impact measures (rather than to other aspects of the evaluation). As a result, the evaluation has relied mainly on stakeholder consultations.

The partial contributions to the online surveys by the Member States (responses covered 22 EU countries) prevented a fully-fledged comparative analysis across the European Union;

Relatively low response rate from DSPs (including micro and small businesses) in all consultation activities, which may result from the ‘light touch approach’ and ex-post supervision towards DSPs. Besides that, as observed during the in-depth interviews with different stakeholders, as DSPs are already complying with several international standards and certifications and they remain free to take the measures that they deem appropriate, they may see the need to comply with the NIS Directive as less relevant.

Limited evidence on the actual impacts of the Directive, since the Directive has been implemented by the Member States only as of 2018, and some of them have experienced delays in its implementation. At the same time, the risk of drawing invalid conclusions has been mitigated by the online surveys and in-depth interviews with national competent authorities, SPOCs and CSIRTs.

The above-mentioned issues limited the analysis especially in relation to the ‘EU added-value’, ‘effectiveness’ and ‘efficiency’ evaluation criteria. However, conclusions have been drawn based on the triangulation and validation of findings from desk research and the consultation activities with stakeholders against the different evaluation criteria.<sup>225</sup>

### **e) ANALYSIS AND ANSWERS TO THE EVALUATION QUESTIONS**

By comparing the baseline situation with the implementation state of play, it is possible to study to what extent the outputs and outcomes that can be observed (see the intervention logic described in *Figure 1* above) correspond to the expectations concerning what the Directive should achieve, i.e. a high common level of security of network and information systems within the European Union. The below analysis is based on the five evaluation criteria: relevance, EU added value, coherence, effectiveness and efficiency.

#### **Relevance**

The evaluation criterion of relevance assesses how the objectives of an EU intervention correspond to the current needs and problems in society, as well as to the wider EU policy priorities. Under this criterion, the analysis should identify if there is any

---

<sup>225</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

mismatch between the objectives of the intervention and the needs or problems, e.g. incorrect assumptions or any change in the circumstances.

As laid down in Article 1(1), the overall aim of this legislation is to achieve a high common level of security of network and information systems within the European Union so as to foster trust and cooperation among the Member States and improve the functioning of the internal market. This translates into several specific objectives. In addition to the objectives of setting out national frameworks and achieving cooperation at EU level, the analysis verifies whether all the relevant sectors and sub-sectors of OES as well as all types of DSPs that would be considered essential for the smooth functioning of the economy and society and covered under the scope of the Directive.

*Evaluation question:* To what extent are the original objectives of the NIS Directive still pertinent in relation to the evolving needs, technological advances and problems at both national and EU levels?

The results of the Commission consultations show that overall the specific objectives of the NIS Directive are relevant. Respondents consider as most relevant the objectives to take appropriate measures to prevent and minimise the impact of incidents (Article 14(2) and 16(2) and to take appropriate and proportionate measures to manage the cybersecurity risks (Article 14(1) and Article 16(1)). Also very relevant are the objectives to improve strategic cooperation and the exchange of information among Member States (Article 1(2b), Articles 11 and 12) and adopt a NIS strategy and notify significant incidents. NCAs find it relevant to contribute to the development of trust and confidence between Member States and to set up inter-institutional cooperation at national level to fulfil the obligations under the Directive.

Operators of essential services, DSPs and NCAs believe that the issues, which were considered most prominent at the time of adoption of the NIS Directive are still very relevant until today. Such are the increasing magnitude, frequency and impact of cybersecurity attacks and incidents, which could cause major damage to the economy of the Union, the insufficient capabilities in the Member States and different preparedness, leading to fragmented approaches across the EU.

However, the growing interconnectedness and the changing threat landscape also resulted in legal gaps and uncertainties stemming, among others, from the implementation of the Directive at national level. The inconsistencies in the national implementations of the Directive put in question the achievement of a level playing field for some operators within the Internal Market.

For instance, as explained above in Section c) on implementation (OES identification), there is a considerable lack of harmonisation across the Union when it comes to the identification of OES. Stakeholders agree that the minimum harmonisation approach towards OES leaving an important degree of flexibility to Member States in the transposition and thus leading to very diverse results, is one of the key shortcomings of the NIS Directive. The result is a misalignment of security requirements and incident notification requirements for OES across Member States.

The minimum harmonization approach also led to the inclusion of additional sectors and corresponding sub-sectors beyond the scope of the Directive considered nationally sensitive and potentially vulnerable to cyber-incidents. The consultation confirmed that most NCAs believe that the Annex II of the NIS Directive does not cover all relevant

sectors and subsectors when it comes to the provision of services essential for the economy and society as a whole.<sup>226</sup> For instance, the majority of the competent authorities judged (“to a great extent”) that the sectors electricity generation, wastewater, emergency services, food supply and public administration could be added.

Also, due to the significant interdependencies with the other sectors under the NIS Directive, the telecoms sector, currently regulated under the European Electronic Communications Code (EECC), is considered as meriting to be part of the scope of the NIS Directive, to ensure coherence and consistency with the NIS Directive provisions.

Comparing the NIS Directive objectives and the current needs and problems in the area of cybersecurity within the EU, there are new challenges coming from the evolving digital transformation of our society. In view of the growing interconnectedness and interdependencies between sectors and providers, according to a majority of OES, the main criteria to identify emerging essential sectors and/or services that need to fall within the scope of the Directive are the reliance on the respective sector or service of other essential sectors (or a number of essential services) expressly mentioned within the scope of the Directive.<sup>227</sup> This leads to the need for introducing policies related to supply chain cybersecurity management. The increasingly connected ICT infrastructures, the rising number of connected devices through IoT and industry 4.0, the growth of 5G networks raise concerns regarding vulnerabilities in the supply chain could have cascading impacts across multiple critical infrastructures and services.

Regarding DSPs, the open public consultation showed that there was no agreement among stakeholders whether Annex III of the NIS Directive covers all relevant types of digital services, as around a third of respondents disagreed while 26.7% ‘agreed’ with the statement. The agreement varied also considerably between the groups, with agreement ranging from only 14.3% (NCAs) to 50% (Citizens). More generally, a third of the operators and DSPs believe there is insufficient consideration of critical internet-related technologies/entities (e.g. data centres and content delivery network (CDN) or geolocation services, social media platforms are not covered), which may render the entire digital ecosystem vulnerable. The majority of NCAs consider as a main shortcoming the limitations in determining the DSPs falling under the scope of the Directive, the light-touch approach when it comes to supervision of security measures and incident reporting, as well as the insufficient clarity about the establishment of jurisdiction for DSPs. Incident reporting as a result of high thresholds and the enforcement measures are also considered as insufficient and are also subject to criticism by the NCAs.<sup>228</sup> The limited information sharing between Member States, potentially hampering the effective handling and prevention of incidents, a misalignment of security requirements for operators of essential services across Member States, insufficient voluntary incident reporting schemes are among the other main identified shortcomings.

---

<sup>226</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>227</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>228</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

## Coherence

This criterion investigates how different actions of the NIS Directive fit together and within a wider framework (e.g. other EU initiatives). The analysis of *external coherence* highlights areas where there are synergies or tensions among different EU interventions. Meanwhile, the analysis on *internal coherence* evaluates how the various elements of the Directive work together in order to achieve its objectives<sup>229</sup>.

*Evaluation question:* To what extent does the NIS Directive fit well within the wider EU cybersecurity policy, and, more specifically, is it coherent with other EU interventions in the field of cybersecurity (incl. in specific sectors or with regard to security of products) and critical infrastructure protection?

For this analysis, the evaluation looked into the different definitions and concepts provided by the NIS Directive and analysed how these are coherent to other EU interventions such as Directive (EU) 2018/1972 (EECC)<sup>230</sup>; Directive 2008/114/EC (ECI Directive)<sup>231</sup>; Directive 2015/2366/EU (PSD 2)<sup>232</sup>; Regulation (EU) 2019/881 (Cybersecurity Act)<sup>233</sup>; Regulation (EU) No 910/2014 (eIDAS Regulation)<sup>234</sup>; and Regulation 2016/679 (GDPR)<sup>235</sup>. The analysis revealed that there should be a better alignment of requirements (e.g. reporting authorities, thresholds, time-frame, and penalties), between the NIS Directive and other EU legislation, especially considering risks such as double jeopardy (e.g. imposition of administrative fines under different regimes in case of non-compliance). For instance, there are overlapping reporting obligations with the GDPR since, while many security incidents involve some personal data, the relation between the two instruments – NIS Directive and GDPR - is not explicitly clarified. Moreover, conflicting reporting obligations with the eIDAS Regulation may arise when digital certificates are used for authentication in services that fall under the scope of the NIS Directive, while duplicated reporting schemes exist with PSD2<sup>236</sup> as payment service providers shall report operational or security incidents to

<sup>229</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)

<sup>230</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, pp. 36-214.

<sup>231</sup> Council 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, OJ L 345, 23.12.2008, pp. 75-82.

<sup>232</sup> Directive (EU) 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, OJ L 337, 23.12.2015, pp. 35-127.

<sup>233</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, OJ L 151, 07.06.2019, pp. 15-69.

<sup>234</sup> 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, OF L 257, 28.08.2014, pp. 73-114.

<sup>235</sup> Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016, pp. 1-88.

<sup>236</sup> The Commission Proposal for a Regulation on Digital Operational Resilience for the Financial Sector or the Digital Operational Resilience Act (DORA) adopted on 24 September 2020 amending PSD2



their competent authorities and to their respective NIS competent authority as well. The different reporting schemes that overlap however usually have different aims, thresholds and requirements, and therefore are not substitutable. As such, the findings from the coherence analysis suggests that instead of benefitting from synergies by identical requirements, different reporting mechanisms may hamper the aims of these instruments.<sup>237</sup>

Furthermore, the NIS Directive presents a number of legal concepts, which allow for interpretation and so provide large room for manoeuvre to Member States to decide how to reach a high level of security of network and information systems. For example, the definitions of ‘significant’ or ‘substantial’ effect; ‘appropriate and proportionated technical and organisational measures to manage the risks’ are not precisely elaborated in the Directive. Although the majority of stakeholders replying to the online surveys declared that the concepts and definitions provided in the NIS Directive are clear enough, respondents flagged that the identification of OES and definition of DSPs are the main unclear points of the Directive and could impact the level of awareness of their obligations including insufficient clarity of the provisions on how to determine the ‘significance of the impact of an incident’. They mentioned that more clarity regarding provisions on ‘incident notification’ and ‘reporting requirements’ would be welcome. Lastly, while the Directive aims to achieve a high ‘common’ level of security of network and information systems’, it set minimum standards by legal concepts such as ‘state of the art’, ‘appropriate technical and organisational measures’, ‘effective, proportionate and dissuasive’ penalties, thus leaving room for various national interpretations risking to achieve diverging standards.

Finally, the information gathered indicates that the NIS Directive has made a positive contribution to the establishment of a common high level of security of network and information systems and thus upscaling capacities, cooperation and risk management practices across the EU Member States. Prior to its adoption, there was no regulation for cybersecurity in some Member States, yet all of them are now complying with the minimum requirements imposed by the NIS Directive. However, evidence suggests that there are significant discrepancies in the obligations imposed on OES, as well as in the enforcement of the Directive across Member States, and uncertainty about scope and jurisdiction for DSPs. This suggests that a sufficient level playing field particularly important for cross-border operators, has not yet been achieved.<sup>238</sup>

### **EU Added Value**

This criterion investigates the changes of the EU intervention compared to what could reasonably have been expected from national and regional actions<sup>239</sup>.

*Evaluation question:* What has been the added value of the NIS Directive compared to what could have been achieved by Member States at national or regional level?

---

aims at streamlining incident reporting obligations for the financial sector among other things. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A595%3AFIN>

<sup>237</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>238</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>239</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)

The evidence suggests<sup>240</sup> that the Directive has played an important role in creating a cybersecurity framework and, therefore, in overcoming concerns regarding national sovereignty in this domain by strengthening the security of network and information systems across the Union without hindering or prejudicing the respect of the subsidiarity and proportionality principles.

There was an increase in the number of national cybersecurity strategies across the EU Member States since the implementation of the NIS Directive. The reliability and security of network and information systems directly contributes to the overall functioning of the Internal Market. This is one of the main priorities of the EU (Article 114, TFEU), and without a harmonised set of cybersecurity rules at EU level, it is unlikely that improvement in cybersecurity capacity and preparedness would be achieved in the Member States.

Nonetheless, the consulted stakeholders confirmed that there is room for improvement in the provisions of the NIS Directive in relation to the creation of a more coherent cybersecurity framework across the Union. There is the need to harmonise the Member States' methodologies to identify OESs, their definition, and the incident thresholds, as asymmetries in relation to OESs dispositions create a risk of fragmentation in the internal market. Similarly, it appears that a certain degree of inconsistency exists in the national application of the Directive with regard to Article 1(3) leading to the identification of OESs where sector-specific rules apply (e.g. in the telecoms sector) and insufficient OES identification in some of the sectors listed in Annex II. The role of the NIS Cooperation Group could also be strengthened to promote a common understanding on how to coherently implement the Directive amongst Member States.<sup>241</sup>

Overall, the implementation of the Directive allowed Member States to enjoy a series of direct and indirect benefits, such as increased safety for all stakeholders, increased information sharing, increased information availability, among others. However, when comparing challenges at the time of the NIS Directive adoption and current and future issues and threats, further EU action is and will be required. Among the most pressing upcoming challenges are (i) the necessary development of cybersecurity skills in the EU; (ii) the need of cybersecurity standardisation efforts; (iii) the necessity to pursue EU efforts to strengthen incident response capabilities, procedures, processes and tools to avoid eventual repetitions or loopholes; (iv) and the consolidation, planning and work ahead on EU capabilities to ensure cybersecurity resilience of current and upcoming technologies (e.g. 5G networks, artificial intelligence, internet of things, blockchain).

To sum up, the NIS Directive has contributed to the achievement of results that could not have been attained at the national level. In this sense, the continuation of the EU action is needed to further ensure a high common level of security of network and information systems across the Union for the European society and its citizens.<sup>242</sup>

---

<sup>240</sup> E.g. 57% of the Competent Authorities agree 'to a great extent' on the fact that the NIS Directive improved cooperation and the exchange of information among Member States.

<sup>241</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>242</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

## **Effectiveness**

This criterion intends to (i) assess the extent to which the general and specific objectives of the NIS Directive have been achieved; (ii) identify any significant factors that may have contributed to, or inhibited progress towards, meeting these objectives; and (iii) investigate any negative or positive changes produced beyond the intended effects of the NIS Directive<sup>243</sup>.

*Evaluation question:* To what extent and why has the NIS Directive been an effective instrument for achieving a high common level of security of networks and information systems within the EU?

Evidence indicates that the full transposition of the Directive by Member States has generally improved the situation of EU cybersecurity. As observed, stakeholders agree that both the adoption of a national strategy and the designation of one or more national competent authorities, CSIRTs and of a SPOC were effective in achieving a higher level of security of network and information systems. The adoption of the national cybersecurity strategies gave impetus to the implementation of a series of concrete policy actions such as the definition of a risk-assessment plan, a governance framework to achieve the objectives of the national strategy and the identification of measures related to cybersecurity capacity building such as preparedness, response and recovery. This legal provision helped the countries with less capacity to make a substantial step forward in cybersecurity preparedness, ensuring a high level of security in their territory.

However, shortcomings in the implementation may hinder the full achievement of the objectives and expected results of the NIS Directive. For instance, significant differences remain concerning the implementation of risk assessment procedures, the availability of reporting platforms for incidents and the allocation of resources and staffing to designated national competent authorities.

Differences also exist among Member States with respect to the designation of competences at the national level (e.g. centralised vs. decentralised approach). Moreover, there are significant divergences in the ability of competent authorities to accomplish their tasks due to different levels of allocation of adequate financial and human resources. Most stakeholders that took part in the consultation agree that the lack of adequate financial resources and staffing emerged as one of the most relevant challenges that national competent authorities have faced in the implementation of the NIS Directive.

As far as the effectiveness of the Directive in fostering CSIRTs ability to comply with requirements and tasks is concerned, the evaluation shows that although a minimum maturity level was met, the level of operational capacity and reliability of national CSIRTs also greatly varies. In this respect, resources' limitation or lack of technical capacity may create challenges for CSIRTs to meet all the responsibilities defined in Annex I of the NIS Directive while having to deal with incidents of national priority. National CSIRTs are not always considered to lead in raising awareness on threats among the private sector. Instead, operators often turn to commercial organisations providing early warning and incident response capabilities. Finally, because the role and

---

<sup>243</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)

range of national CSIRTs diverges, their cooperation with national law enforcement, the SPOC, other competent authorities, OES and DSPs have also been uneven. According to the OES' responding to the online survey, the main challenges faced when cooperating with the national competent authorities and national CSIRTs are related to the lack of understanding about their field of activity, the focus on national critical infrastructure rather than cross-border dependencies, and the lack of support for information sharing, such as a mechanism for authorities to share information with established private sector initiatives under public-private partnership programmes (see above in Section on *Implementing and transposing measures*).<sup>244</sup>

Regarding the effectiveness of SPOCs in fulfilling their tasks as members of the wider national institutional cybersecurity framework, most respondents considered that SPOCs are effective in coordinating issues related to the security of network and information systems and cross-border cooperation at Union level. However, some stakeholders believe that SPOCs and CSIRTs tasks are overlapping in some Member States and therefore the liaison function of these entities should be clarified. Respondents also explained that SPOCs should be given more responsibilities than just transmitting information between different stakeholders. They also pointed out that it is common that important information is missed or not distributed correctly. A high number of competent authorities' respondents declared that they have limited overview over the level of cooperation between NCAs and SPOCs in another Member State.

With respect to the effectiveness of cooperation at the EU level, while the Cooperation Group has facilitated the exchange of information and has offered guidance for Member States consultation in cases of OES operating across borders, few members actually use the cross-border consultation instrument. The evaluation also shows the need for more structured cooperation and improved communication between the Cooperation Group and the CSIRTs Network.

Another important factor which stood in the way of fully achieving the NIS Directive objectives is the variation in methodologies to approach the definition of essential services, the identification of OES, and the specification of thresholds. These discrepancies hinder the management of cyber-dependencies for OES operating across different Member States limiting the effectiveness of the NIS Directive and raising concerns about the proper enforcement at national level and the consistent implementation of cybersecurity measures across the EU.

The evaluation also analysed the Member States' ability to establish security requirements and to impose incident reporting requirements on OES and DSPs.

Minimum-security requirements vary across Member States, ranging from setting a minimum length for passwords in absence of two-factor authentication to more general requirements. In this respect, there is the need to define similar security objectives for each sector, especially for OES with cross-border activities, and to consider specific measures by market-operators of different size, especially SMEs.

With regard to incident reporting requirements, the differentiation in schemes is not optimal for cross-border providers, which are often subject to different notification

---

<sup>244</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

regimes. Also, under the current reporting regime, cybersecurity authorities are unable to acquire knowledge relative to incidents below a certain threshold. Indeed, only in few Member States voluntary reporting is envisaged and encouraged through, for instance, reporting near misses. In order to promote incident reporting it is thus necessary to streamline the definition of a significant incident and /or to adjust thresholds.

Thresholds and modalities of reporting vary substantially across Member States. It can be observed that in some countries thresholds do not exist at all while in some others they are extremely detailed and/or vary by sectors. Such multitude of sectoral approaches challenge a common regulatory approach in the EU and hamper the activity of cross-border operators.

In relation to the effectiveness of the NIS Directive regarding DSPs, a majority of the limited number of DSP respondents<sup>245</sup> consider that it has been effective in achieving its overall objectives. At the same time, the majority of national competent authorities<sup>246</sup> consider as ineffective the approach for determining the DSPs falling under the scope of the Directive stemming among others from an insufficient clarity about the establishment of jurisdiction for DSPs, as well as the ineffective light-touch approach when it comes to supervision of security measures and incident reporting. Another criticism by national competent authorities is that, as a result of high incident reporting thresholds, very few incidents are being reported, also failing to meet the set objectives.

Finally, with respect to penalties, there is great variation in magnitude across Member States and their application. Penalties vary by sector, by entity, by type of incident, among others. The effectiveness and dissuasiveness of some of the maximum penalties provided for in some Member States is also questionable. Moreover, Member States to date have never applied any type of penalties. This situation clearly calls for a specific intervention to align the penalties across Member States.<sup>247</sup>

### **Efficiency**

This criterion considers the relation between the resources used by the intervention and the changes that it generated. Under this criterion, the analysis looks at the costs and benefits of the EU intervention as they accrue to different stakeholders to evaluate whether the benefits are achieved at a reasonable cost and the costs are proportionate to the benefits.<sup>248</sup>

*Evaluation question:* To what extent have the effects of the NIS Directive been achieved at a reasonable cost?

The results of the targeted consultation activities concerning the costs and benefits of the NIS Directive have highlighted a lack of quantitative data. The missing estimates of costs and benefits is due to four main reasons: (i) data are not available as the Directive has only recently been implemented; (ii) the reluctance of stakeholders to share such data, (iii) the difficulty in attributing the costs and benefits of new cybersecurity measures

<sup>245</sup> Overall 9 DSPs (including trade associations) replied to the targeted survey and 16 DSPs (including 3 trade associations) replied to the Open Public Consultation.

<sup>246</sup> 46 NCAs replied to the targeted survey and 14 NCAs replied to the Open Public Consultation.

<sup>247</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>248</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)

directly to the NIS Directive, and (iv) the non-easily quantifiable costs and benefits, such as the reduced number of cybersecurity incidents or the increased compliance costs.

Despite the lack of estimates that equally concerns costs and benefits, it is possible to draw some partial conclusions. Analysing the findings of the targeted consultations related to the costs coming from the NIS Directive, it is evident that the respondents have expressed common views, reporting that they did not incur significant operational, administrative, and compliance costs. The costs that the respondents flagged as the most relevant are compliance costs and, in particular, the duplication of efforts and the time invested to comply with different European legislation, imposing different reporting obligations to different authorities, timelines, and criteria. However, the duplication of reporting requirements due to the lack of external coherence cannot be reported as a direct cost of the NIS Directive.

In regard to the benefits, the results of the targeted consultation activities show that the respondents have experienced additional benefits coming from the NIS Directive, such as the improved security for the functioning of economy and society and the increased trust and cooperation among the Member States. The perceived benefits vary across stakeholders. Competent authorities gave mainly positive replies in relation to the benefits coming from the NIS Directive, while OES and DSPs experienced one main benefit - a reduced impact of cybersecurity incidents for OES, and increased trust in the digital economy and the internal market for DSPs. However OES and DSPs were more critical in relation to other types of benefits, i.e. decreased costs of security incidents, including malicious attacks and a reduced number of NIS incidents.

Finally, the respondents' answers concerning the proportionality of the costs and benefits of the NIS Directive are positive, with all stakeholder groups considering the cost proportionate to the benefits to a great or to a moderate extent. The stakeholder group that is more critical about the proportionality of costs and benefits is the OES in the banking and financial market infrastructure sectors. This is partly due to the fact that entities in these two sectors considered themselves already compliant with requirements similar to those imposed by the Directive before the entry into force of the NIS Directive.

Overall, the results of the consultation activities tend to show that the costs of the Directive are reasonable and proportionate to the benefits achieved. However, no conclusive consideration can be done in relation to the costs and benefits, as the lack of estimates limits the analysis of the efficiency of the NIS Directive.<sup>249</sup>

## **f) CONCLUSIONS**

Overall, the NIS Directive can be considered as a major first step in reaching the objectives to raise the common level of cybersecurity amongst the Member States. The NIS Directive has ensured the completion of national frameworks by defining the national cybersecurity strategies, establishing national capabilities and implementing regulatory measures covering the critical infrastructures and actors identified by each Member State. The Directive has also greatly contributed to developing the cooperation at the EU level within the frameworks of the Cooperation Group and CSIRTs Network.

---

<sup>249</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

However, the growing interconnectedness and dependence on digital technologies as well as the expanding threat landscape have intensified the need for a strong EU response. Member States capabilities are still unequal and resources are often insufficient leaving certain competent authorities in a position, in which they can no longer effectively fulfil their obligations under the Directive. In view of the minimum harmonization requirements imposed by the Directive, Member States have taken diverging approaches when identifying OES and prescribing security requirements and incident reporting obligations. This has led to discrepancies and gaps in the implementation of the Directive and has failed to achieve a sufficient level playing field for operators and in particular cross-border players, within the Union. The sectors identified beyond the scope of the Directive also demonstrate the need to expand the scope to further sectors that are considered essential and equally vulnerable to cyber threats. In view of DSPs' increasing role in the digital economy, the current light-touch regime, which has demonstrated its limitations, merits a re-evaluation and a clarification regarding the type of providers that fall in the scope, the process to establish DSP's jurisdiction within the Union and the national competent authorities' ex-ante supervisory powers. Information sharing has remained limited both from operators and DSPs as between national competent authorities. The high incident reporting thresholds leading to only few reportable incidents stay in the way of developing a comprehensive view of the threat landscape. Despite the success of the Cooperation Group, due to the voluntary nature of information exchanges between the authorities, no systematic information sharing between Member States has been taking place. This is the case also in situations with direct cross-border implications. Therefore, to be able to keep in pace with technological and threat landscape evolution and to achieve the original objectives of the NIS Directive and make it future-proof, the discrepancies between the Member States transposition and legal gaps need to be removed.



EUROPEAN  
COMMISSION

Brussels, 16.12.2020  
SWD(2020) 345 final

PART 3/3

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT REPORT**

*Accompanying the document*

**Proposal for a Directive of the European Parliament and of the Council  
on measures for a high common level of cybersecurity across the Union, repealing  
Directive (EU) 2016/1148**

{COM(2020) 823 final} - {SEC(2020) 430 final} - {SWD(2020) 344 final}



## Table of Contents

Annex 6: Overview of selected results of the targeted surveys conducted by the NIS review study .....	5
Annex 7: Overview of related cybersecurity legal acts and policy measures .....	45
Annex 8: Overview of policy options .....	55
Annex 9: Cross-sector and cross border propagation of incidents .....	63
Annex 10: Extract from the interim results of the NIS review study on a modelling for costs and benefits.....	65
Annex 11: List of indicators to monitor high-level progress towards general objectives.....	67
Annex 12: List of indicators to monitor progress towards specific objectives .....	70

## Glossary: acronyms

<i>Term or acronym</i>	<i>Meaning</i>
AI	Artificial Intelligence
CDN	Content delivery network
CSIRTs	Computer Security Incident Response Teams
CyCLONe	European Cyber Crises Liaison Organisation Network
DDoS	Distributed Denial of Service
DEP	Digital Europe Programme
DESI	Digital Economy and Society Index
DNS	Domain Name System
DORA	Digital Operational Resilience Act for the financial sector
DSP	Digital service provider
EASA	The European Union Aviation Safety Agency
ECCSA	European Centre for Cybersecurity in Aviation
ECI Directive	Directive on the identification and designation of European critical infrastructures
ECJ	European Court of Justice
EECC	European Electronic Communications Code
EMSA	European Marine Safety Agency
eIDAS (Regulation)	Regulation on electronic identification and trust services for electronic transactions in the internal market
ENISA	The European Union Agency for Cybersecurity

GDPR	General Data Protection Regulation
IaaS	Infrastructure as a service ( <i>cloud service model</i> )
ICS	Industrial control system
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union: The United Nations specialised agency for information and communication technologies
IXPs	Internet Exchange Points
JRC	European Commission's Joint Research Centre
LOTL	European List of eIDAS Trusted Lists
OES	Operator of essential services
OPC	Open public consultation
MeliCERTes	Cybersecurity Digital Service Infrastructure Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs
NACE	Statistical Classification of Economic Activities in the European Community
NIS Directive	Directive concerning measures for a high common level of security of network and information systems across the Union
NIST	National Institute of Standards and Technology – US Department of Commerce

PaaS	Platform as a Service ( <i>cloud service model</i> )
PPP	Private Public Partnership
ROSI	Return of Security Investment
SaaS	Software as a Service ( <i>cloud service model</i> )
SME	Small and medium-sized enterprises
SPOC	Single Point of Contact
TFEU	Treaty on the Functioning of the European Union
TLD	Top-level domain

## ANNEXES

### ANNEX 6: OVERVIEW OF SELECTED RESULTS OF THE TARGETED SURVEYS CONDUCTED BY THE NIS REVIEW STUDY

Throughout July-September 2020, the NIS review study conducted targeted surveys for three categories of stakeholders: competent authorities, operators of essential services and digital service providers. The surveys had: 46 respondents on the side of competent authorities, 49 for operators of essential services and 9 for digital service providers.

This annex provides a summary of the results of the targeted surveys, as well as extracts of these results, as they were referred to throughout the impact assessment report. The results and charts were prepared by the Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665 – implemented by Wavestone, CEPS and ICF. The final report of the study, due by December 2020/January 2021 was not submitted at the time of the writing of this report.

#### Overview

The targeted consultation consisted of **online surveys** and **in-depth interviews**.

As part of the targeted consultation, the Project Team developed three **online surveys** targeting

- National Competent Authorities (CAs, including CSIRTs and SPOCs),
- Operators of Essential Services (OESs)
- Digital Service Providers (DSPs)

All three online surveys ran between 15 July and 4 September 2020. The questionnaires were tailored to each stakeholder group and were structured following the five evaluation criteria: relevance, effectiveness, efficiency, coherence EU added value.

The questions were grouped according to the main provisions of the NIS Directive exploring context specific aspects which gave the targeted respondent the possibility to provide evidence-based information coming from their experience.

The surveys prepared for OESs and DSPs were also shared with and disseminated through associations or networks of OESs and DSPs, significantly increasing the reach of the surveys through the snowballing technique.

The respondent breakdown was as follows:

**Table 1: Overview of respondents to the targeted surveys**

<b>Respondent group</b>	<b>Total number of responses</b>	<b>Coverage</b>
CAs (CSIRTs, SPOCs)	46	22 out of 27 MS + UK
OESs	49	All sectors in Annex II
DSPs	9	All services in Annex III

*Source: Wavestone*

**In-depth interviews** were conducted between 23 July 2020 and 8 September 2020. A total of 16 interviews were completed with the following stakeholders:

- 4 CAs

- 7 OESs
- 2 DSPs
- 2 EU Institutions and Agencies
- 1 Think-Tank

### **Contextual relevance**

It was noted the increasing interconnectedness and reliance on digital infrastructures, technologies, and online systems, as well as resilience and trust in the supply chain made the NIS Directive all the more relevant in the current contextual settings. To illustrate this, 54% (25 out of 46) of the CAs responding to the targeted survey thought that the NIS Directive is relevant to a great extent in the current context.

The majority of OESs and DSPs respondents agree that all specific objectives of the NIS Directive are still relevant in the current contextual settings.

Across the groups (CAs, OESs, DSPs) the main issues identified with regard to the extent to which EU legislation on NIS still has relevance were:

- the increasing magnitude, frequency and impact of security incidents, and harmful actions;
- the unequal cybersecurity capabilities and preparedness in the Member States;
- the lack of common requirements for OESs and DSPs; and
- the insufficient structured cooperation among relevant actors.

### **Sectoral coverage**

The targeted consultations confirmed that most CAs (31 out of 46, 67% of respondents) believe that the Annex II of the NIS Directive does not cover all relevant sectors and subsectors when it comes to the provision of services essential for the economy and society.

Unlike the CAs, the OESs shared mixed opinions as to whether to add sectors or sub-sectors to the Annex II of the NIS Directive (12 out of 49, 24% of respondents are in favour; 14 out of 49, 29% of respondents are not; and 23 out of 49, 47% do not know). For those who believe sector or sub-sectors could be added in addition to the ones identified by CAs, one additional sector was raised by OESs and is targeted at the elections service (authorities, technology and process) (5 out of 12, 42% of respondents agree ‘to a great extent’).

### **Emerging challenges**

While there was overall agreement that the problems and needs that were considered most prominent when the NIS Directive was adopted are still relevant today and most likely require action at EU level. These problems led to the identification of a series of main needs in the legislation, including:

- implementing security measures to manage cybersecurity risks, and prevent, minimise and notify incidents;
- harmonising the identification process of OESs across the Member States; and
- addressing the ineffective approach for determining the DSPs falling under the scope of the Directive.

## Coherence

### Of the NIS Directive in the EU cybersecurity policy framework

The consultation covered the degree of coherence between the NIS Directive and a set of other EU legislative texts including: Directive (EU) 2018/1972 (EECC); Directive 2015/2366/EU (PSD2 Directive); Regulation (EU) No 910/2014 (eIDAS Regulation); Regulation 2016/679 (GDPR) ; and Regulation (EU) 2019/881 (Cybersecurity Act).

Across all three stakeholder groups, a significant share of the respondents could not pronounce themselves on the degree of coherence between the NIS Directive and other EU legislative texts. The remaining stakeholders consulted across the three groups noted a satisfactory degree of consistency of concepts and definitions between the Directive and the other EU instruments.

However, a better alignment among certain legal instruments could still be reached in relation to definitions, such as the notion of ‘incident’, as well as reporting requirements, which are heterogeneous in terms of reporting authorities, thresholds, timeframe, and penalties.

### Of the NIS Directive concepts and provisions

The majority of CAs responding to the online survey (63%) indicated that the concepts and definitions provided in the NIS Directive are clear enough. However, 35% of the CA respondents held the opposite view and highlighted the definition and identification of OESs and DSPs as the main unclear points.

OESs and DSPs were also surveyed in order to gather their views on any potential clarity issues regarding the concepts and definitions provided within the NIS Directive. The majority of both (63% for OESs and 56% for DSPs) seem to consider concepts and definitions coming from the NIS Directive clear enough.

Overall, although the majority of the respondents to the targeted surveys declared that the definitions provided in the NIS Directive are clear enough, a number of legal concepts featuring in the NIS Directive were judged to entirely clear, e.g. definition of OESs and DSPs; ‘significant’ or ‘substantial’ impact and ‘appropriate and proportionated technical and organisational measures to manage the risks’.

## EU added value

### Of the NIS Directive compared to Member States acting alone

According to the consulted CAs, the NIS Directive achieved results that could not have been achieved by national policies alone:

- 57% of the CAs responding to the online survey (26 out of 46) agreed ‘to a great extent’ on the fact that the NIS Directive improved cooperation and the exchange of information among Member States;
- 46% of the CAs (21 out of 46) also agreed ‘to a great extent’ that the Directive promoted effective operational cooperation through to the creation of a network of national CSIRTs; and
- 35% (16 out of 46) of the CAs agreed ‘to a great extent’ with the fact that the Directive guaranteed minimum capabilities and the establishment of a national framework.

Results for OESs and DSPs were more mixed regarding the added value of the NIS Directive regarding the above aspects. The most critical stakeholder group appeared to be the OESs taking part in the online survey:

- 29% (14 out of 49) of OESs only agreeing ‘to a moderate extent’ with the fact that the NIS Directive created a level playing field for OESs and DSPs across the EU, which could have not been achieved by national polices alone, in terms of security and notification requirements;
- 35% (17 out of 49) of OESs only agreed ‘to some extent’ with the effective implementation and enforcement of security requirements and notifications by OESs and DSPs.
- 41% of OESs (20 out of 49) indicated not knowing whether the NIS Directive improved cooperation and the exchange of information among Member States, and a further 35% (17 out of 49) indicated not knowing whether the creation of a network of national CSIRTs led to more effective operational cooperation.

#### *Added value of the continuation of EU level action*

Across the three stakeholder groups, responses showed that EU level action on NIS brings added value and should be continued when considering that:

- the general objective of the Directive is yet to be fully achieved;
- harmonisation between Member States, despite considerable efforts, remains incomplete, e.g. OESs identification;
- the revision of the NIS Directive is an opportunity to extend its scope to harmonise the EU landscape, e.g. supply chain security, new technologies, public-private partnerships.

#### *Effectiveness*

##### *Achieving a high common level of security across the EU*

Most of the CAs consulted in the targeted survey (92%, 44 out of 46) regarded either ‘to a moderate’ or ‘to a great’ extent to which the overall provisions of the NIS Directive were effective for achieving a high common level of security.

These results are corroborated by the relative majority of consulted OESs and DSPs, although they have shown more mixed opinions on the effectiveness of the Directive in achieving a high common level of security across the EU. In this context, it has been highlighted that while strategies and frameworks are now in place in all Member States, because of the fact that incident handling is different from Member State to Member State – especially in terms on methodologies, skills and practices –effective cooperation is extremely complex.

##### *Enabling Member States to develop effective cybersecurity policies*

The majority of CAs, OESs and DSPs positively assessed the effectiveness of the Directive in allocating power and tasks to national competent authorities, SPOCs and CSIRTs

While the NIS Directive was deemed across the three groups to contribute to the development of effective cybersecurity policies in the Member States, the results reveal that the level of at least some Member States’ cyber maturity could still be improved.



Around two-thirds of the consulted CAs (30 out of 46) still consider at least to ‘some extent’ the insufficient capabilities in the Member States to ensure a high level of security of network and information systems to be relevant and continue to require action at EU level.

#### Security requirements/incident notifications for OESs & DSPs

The Directive was deemed to have contributed to OESs and DSPs effective management of risks posed to the security of network and information systems.

Results however show a need for improvement concerning:

- the misalignment of security requirements and penalties across the Member States;
- the high incident notification thresholds; and
- the highly fragmented supervisory framework.

#### Cooperation at EU level

The Cooperation Group was deemed effective across all three stakeholder groups in assisting Member States in building capacity and exchanging best practices and experiences.

Similarly, the CSIRTs Network was overall deemed to have a positive impact in clarifying actors’ role and responsibilities within the incident response process.

However, respondents frequently highlighted the need for improvements regarding communication and collaboration between the Cooperation Group and the CSIRTs Network.

#### Efficiency

##### Costs

The findings of the online surveys showed that the administrative and compliance costs brought about by the NIS Directive were deemed reasonable by most CAs, OESs and DSPs.

However, stakeholders taking part in the in-depth interviews frequently flagged the duplication of efforts in the implementation of the NIS Directive as having negative implications on costs, both in terms of human resources and time. Duplication was highlighted as a result of efforts undertaken to ensure compliance with multiple legislative texts, which often implies the existence of different reporting authorities, timelines, and thresholds.

##### Benefits

The NIS Directive was overall viewed as having contributed to the setting up of a horizontal framework for the security of networks and information systems at the EU level, triggering the implementation of security measures across the Member States and fostering collaboration and trust within the Union.

According to the results of the online surveys and the in-depth interviews, the main benefits of the NIS Directive were:

- increased trust in the digital economy,
- improved functioning of the internal market
- reduced impact of NIS incidents

## Conclusions

Evidence from the targeted consultation activities reveal that the NIS Directive has relevance given society's ever greater dependency on ICT as well as the evolution of the cyber threat landscape. However, the results also reveal that Member States' capabilities are deemed uneven and sometimes insufficient to respond to cyber threats comprehensively and effectively, including cross-border incidents.

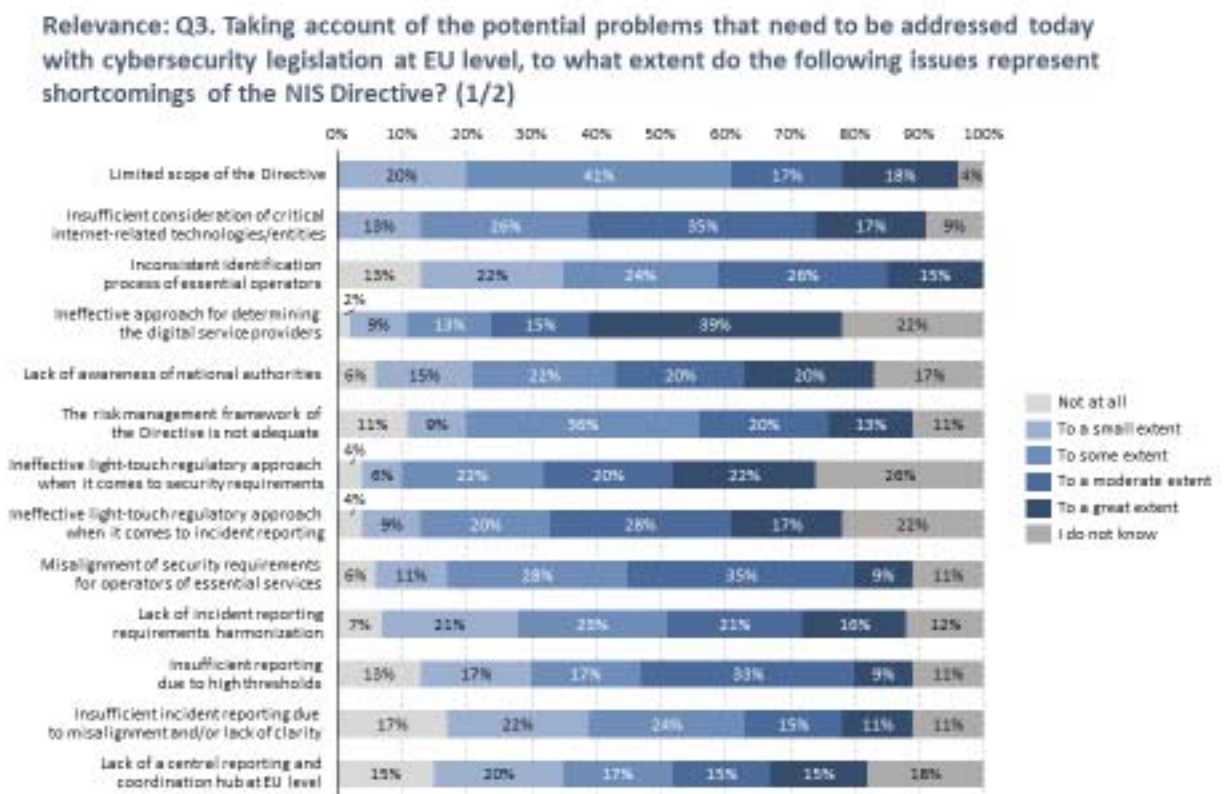
Stakeholders overall recognise that different levels of preparedness within Member States persist, leading to fragmented approaches across the EU for ensuring a high level of cybersecurity.

Based on the results of the targeted consultation, the points to consider in the review of the NIS Directive are as follows:

- lack of harmonisation across the Union when it comes to the identification of OESs
- insufficient consideration of critical internet-related technologies/entities, which may turn the entire digital ecosystem vulnerable
- legal concepts not fully defined, resulting in Member States interpreting them in their own laws which is potentially detrimental to the level-playing field.

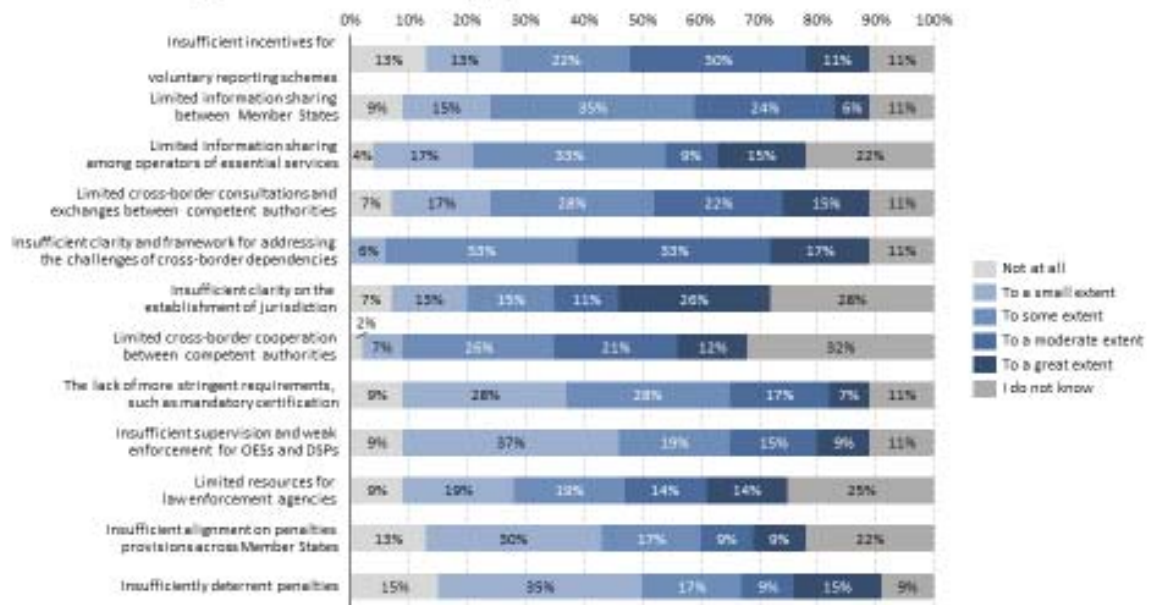
## Illustrative charts on extracts from the results of the survey targeting competent authorities

### *On the shortcomings of the NIS Directive*



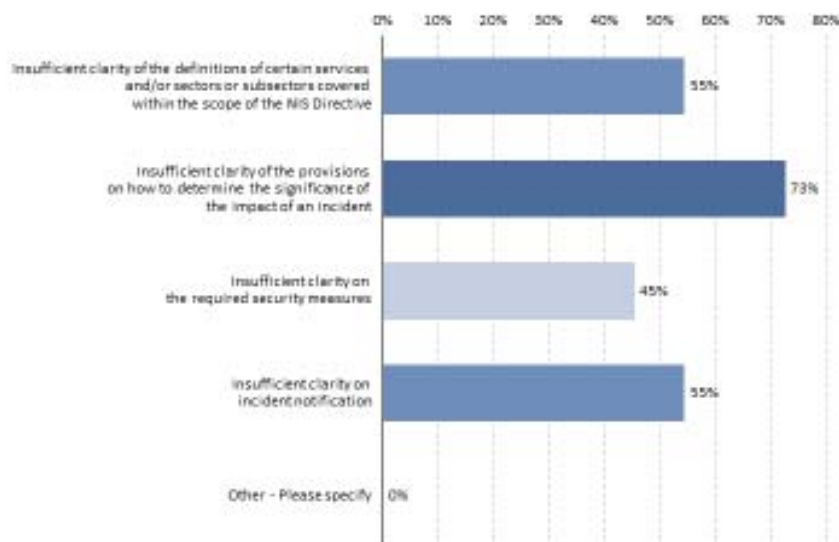
**Source:** Targeted online survey conducted by Wavestone with CAAs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (1/2). N for CAAs: 46

**Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/2)**



Source: Targeted online survey conducted by Wavestone with CAs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/2). N for CAs= 46.

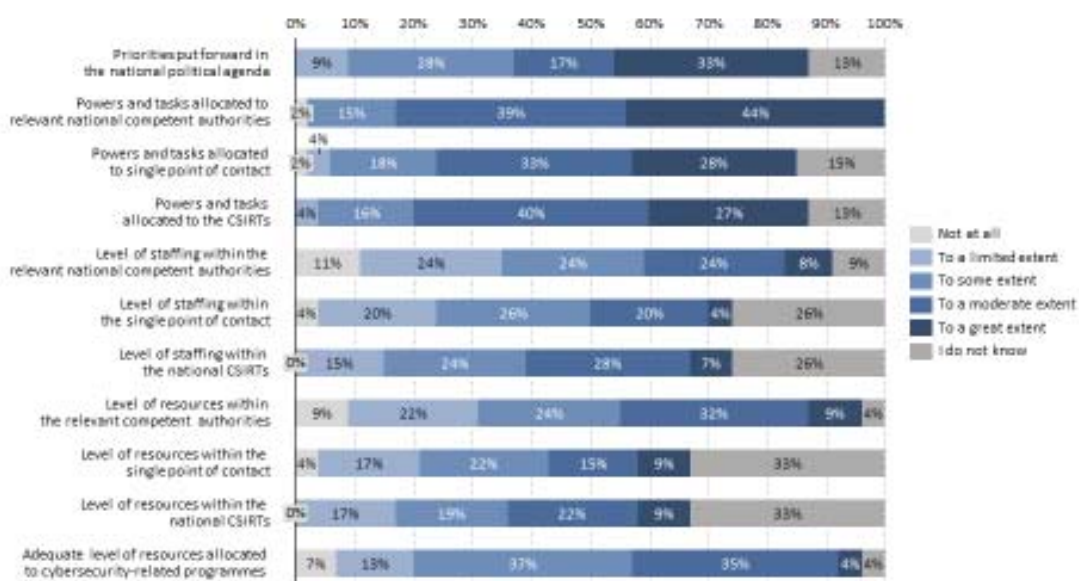
**Coherence: Q10. What are the main problems that could impact the level of awareness of operators of essential services on their obligations?**



Source: Targeted online survey conducted by Wavestone with CAs. Q10. What are the main problems that could impact the level of awareness of operators of essential services on their obligations? N for CAs= 11.

*On the positive impact of the NIS Directive*

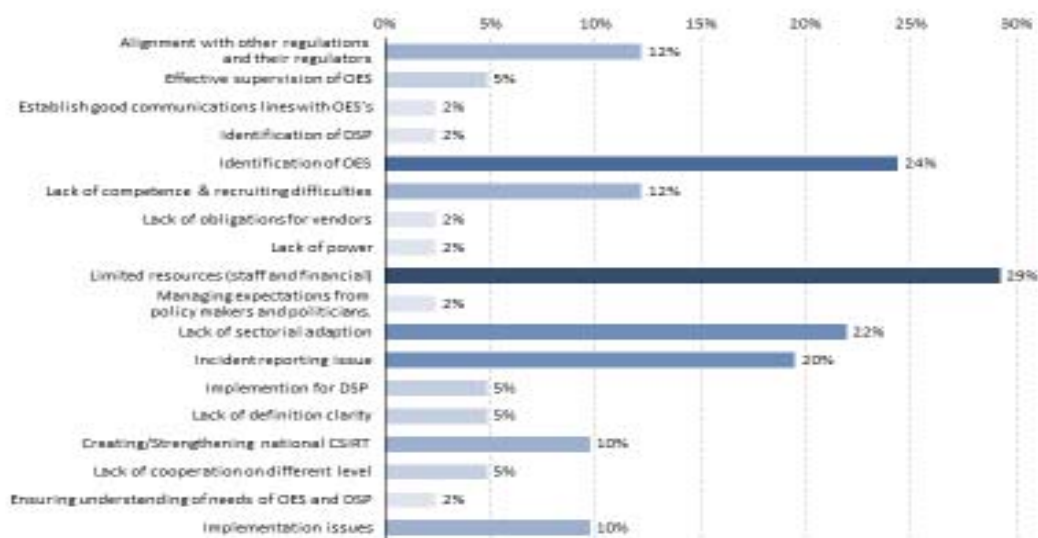
**Effectiveness: Q14. In your view, to what extent has the NIS Directive positively affected the following issues in your country?**



Source: Targeted online survey conducted by Wavestone with CAAs. Q14. In your view, to what extent has the NIS Directive positively affected the following issues in your country? N for CAAs= 46

*On challenges faced in the implementation of the NIS Directive*

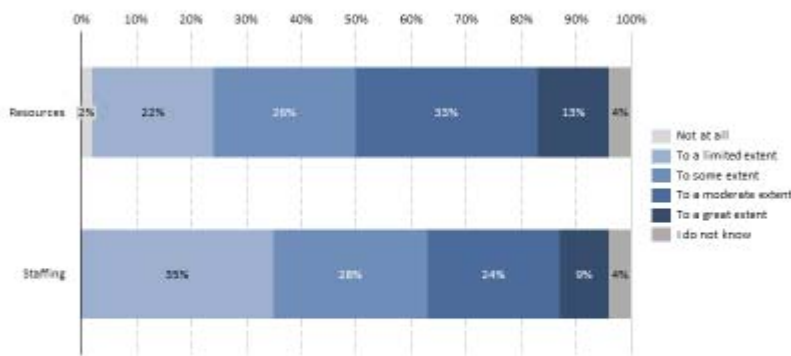
**Effectiveness: Q.20 Which are the most relevant challenges that national competent authorities in your country have faced in the implementation of the NIS Directive?**



Source: Targeted online survey conducted by Wavestone with CAAs. Q.20 Which are the most relevant challenges that national competent authorities in your country have faced in the implementation of the NIS Directive? N for CAAs= 41

## On available resources

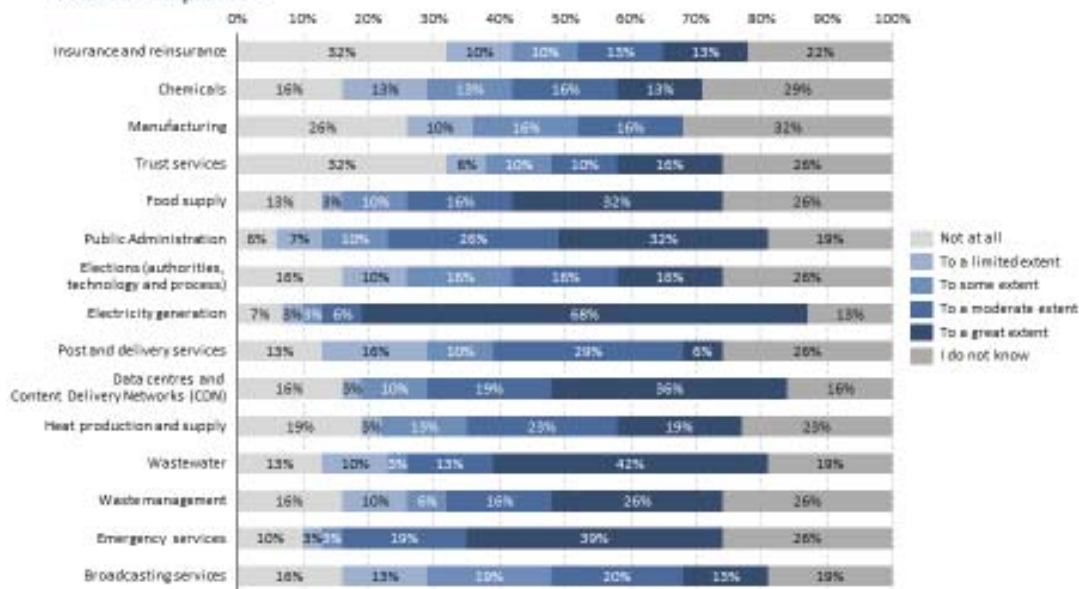
Effectiveness: Q21. Based on your experience, to what extent do national competent authorities dealing with the protection of network and information systems have adequate resources and staffing to fulfil their tasks efficiently?



Source: Targeted online survey conducted by Wavestone with CAs. Q21. Based on your experience, to what extent do national competent authorities dealing with the protection of network and information systems have adequate resources and staffing to fulfil their tasks efficiently? N for CAs= 45

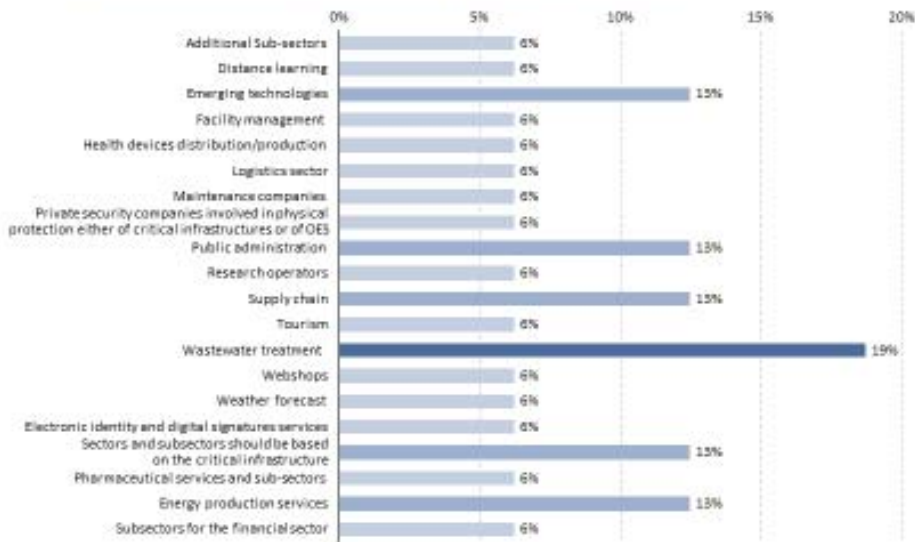
## On the scope of the NIS Directive

Effectiveness: [Conditional Question: if "No" in Q44] Q45. In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile?



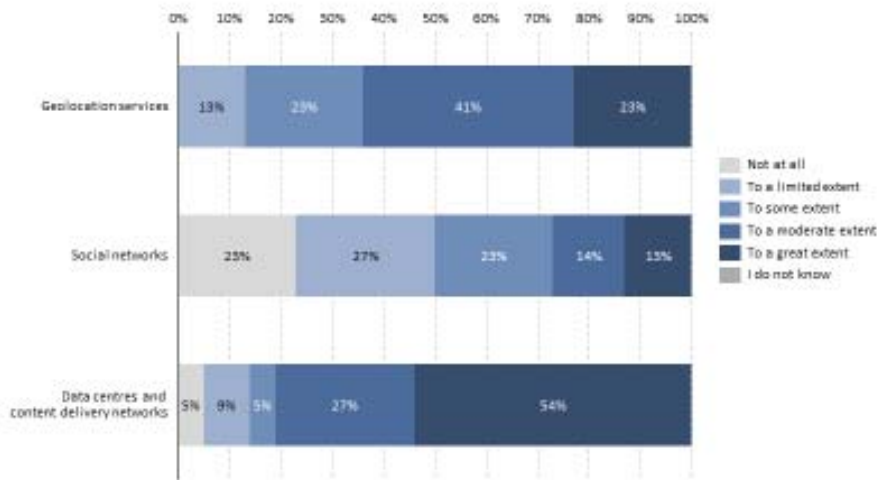
Source: Targeted online survey conducted by Wavestone with CAs. Q45. In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile? N for CAs= 31

Effectiveness: [Conditional Question: if "Yes" in Q46] Q48. Based on your answers to the previous questions, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole?



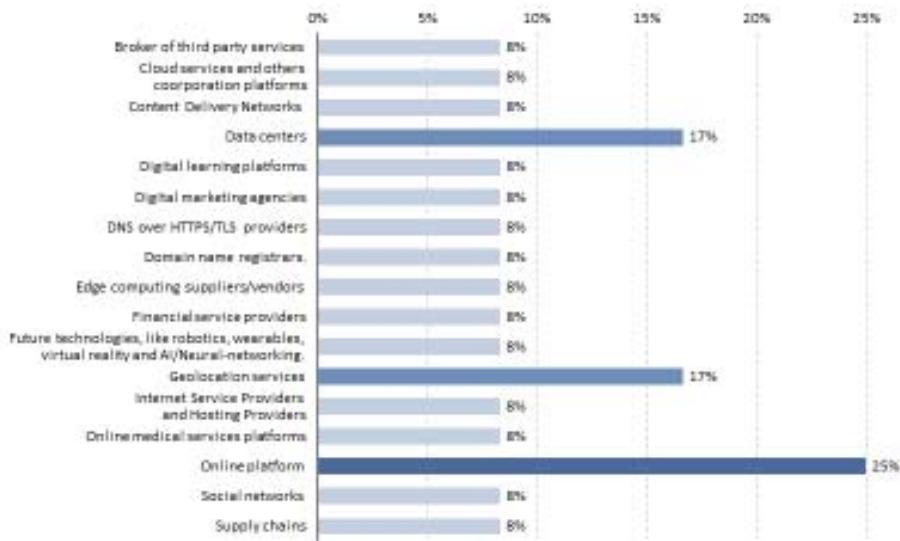
Source: Targeted online survey conducted by Wavestone with CAs. Q48. Based on your answers to the previous questions, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole? N for CAs= 16

Effectiveness: Conditional Question: if "No" in Q55] Q56. In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity-related risk profile?



Source: Targeted online survey conducted by Wavestone with CAs Q56. In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity-related risk profile? N for CAs= 22

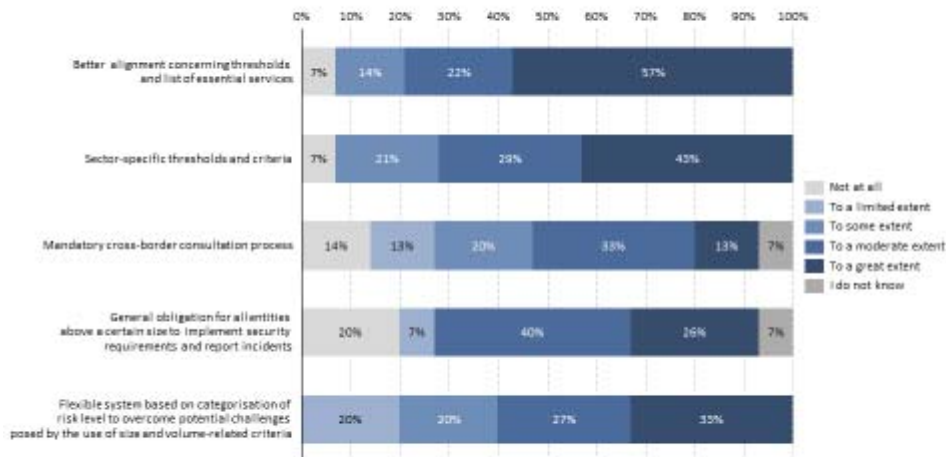
**Effectiveness: [Conditional Question: if "No" in Q55] Q57. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union economy and society?**



**SOURCE:** Targeted online survey conducted by Wavestone with CAs. Q57. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union economy and society? N for CAs= 12

*On identification of OES*

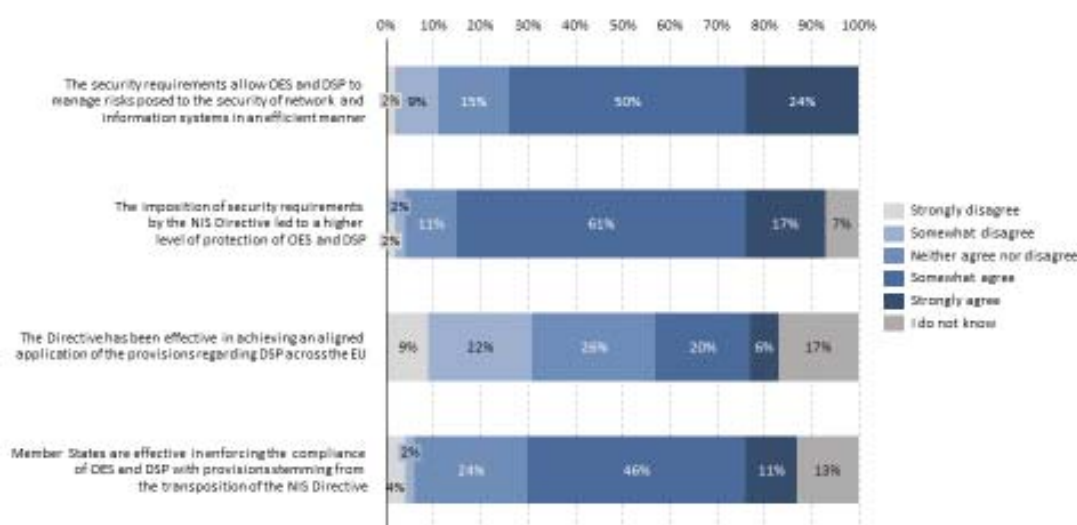
**Effectiveness: [Conditional Question: if "Yes" in Q50] Q51. In your opinion, to what extent could the following aspects improve such identification system?**



**SOURCE:** Targeted online survey conducted by Wavestone with CAs. Q51. In your opinion, to what extent could the following aspects improve such identification system? N for CAs= 15

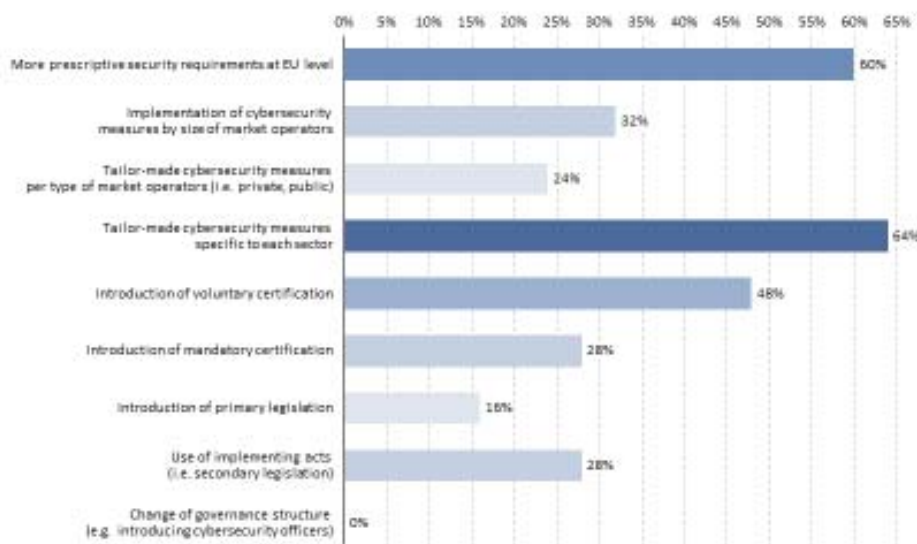
## On security requirements and incident notifications

**Effectiveness: Q59. Thinking about the security requirements and the incident notification provisions laid down in Article 14 and 16 of the Directive, and according your experience, to what extent would you agree with the following statements?**



**Source:** Targeted online survey conducted by Wavestone with CAs. Q59. Thinking about the security requirements and the incident notification provisions laid down in Article 14 and 16 of the Directive, and according your experience, to what extent would you agree with the following statements? N for CAs= 46

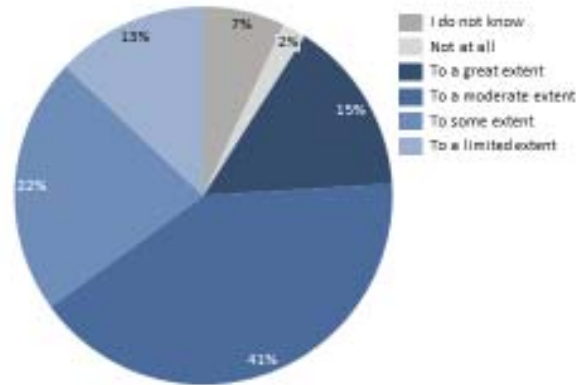
**Effectiveness: [Conditional Question: if "To a moderate extent", "To a great extent" in Q62] Q63. Which of the below options should be considered as means to achieve further alignment of security requirements?**



**Source:** Targeted online survey conducted by Wavestone with CAs. Q63. Which of the below options should be considered as means to achieve further alignment of security requirements? N for CAs= 25

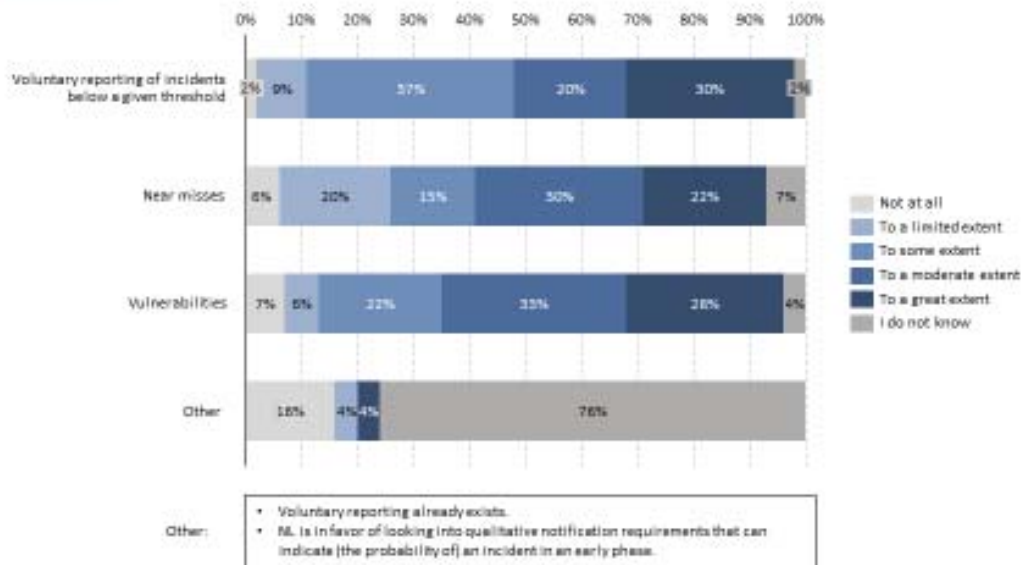


**Effectiveness: Q68. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension?**



**SOURCE:** Targeted online survey conducted by Wavestone with CAAs. Q68. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension? N for CAAs= 46

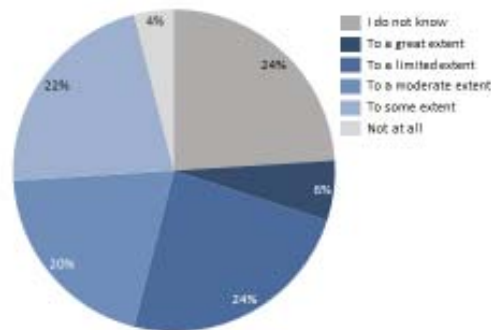
**Effectiveness: Q70. In your opinion, to what extent do you consider those new ways of reporting relevant incidents should be explored such as voluntary reporting schemes, inclusion of additional types of cybersecurity-related incidents such as near misses or vulnerabilities?**



**SOURCE:** Targeted online survey conducted by Wavestone with CAAs. Q70. In your opinion, to what extent do you consider those new ways of reporting relevant incidents should be explored such as voluntary reporting schemes, inclusion of additional types of cybersecurity-related incidents such as near misses or vulnerabilities? N for CAAs= 46

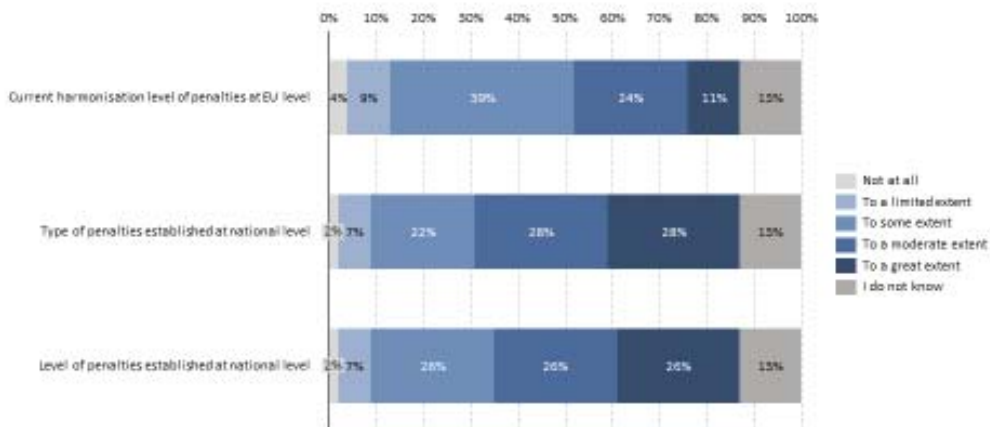
## On supervision and enforcement

**Effectiveness: Q75. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital services providers effective?**



**Source:** Targeted online survey conducted by Wavestone with CAs. Q75. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital services providers effective? N for CAs= 46

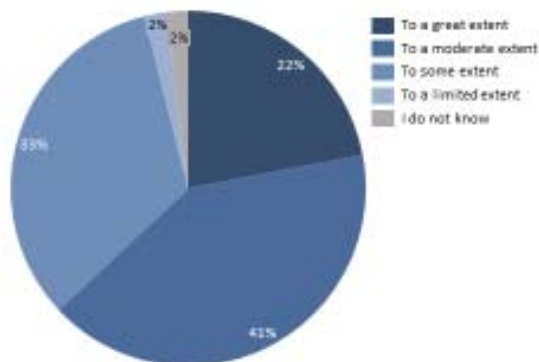
**Effectiveness: Q76. Thinking about penalties both at EU and national level, to what extent do you consider the following measures effective?**



**Source:** Targeted online survey conducted by Wavestone with CAs. Q76. Thinking about penalties both at EU and national level, to what extent do you consider the following measures effective? N for CAs= 46

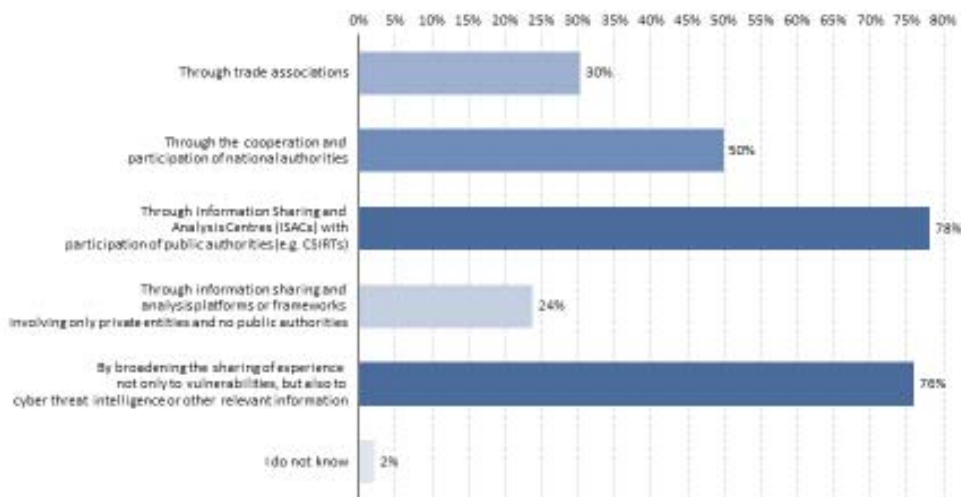
*On information sharing and cooperation*

**Effectiveness: Q83. In your view, to what extent do you think the level of information sharing between the public and the private sectors is effective?**



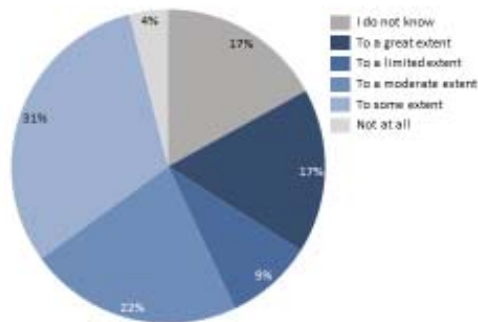
**Source:** Targeted online survey conducted by Wavestone with CAs. Q83. In your view, to what extent do you think the level of information sharing between the public and the private sectors is effective? N for CAs= 46

**Effectiveness: Q85. In your view, how could a better information sharing framework between companies be promoted?**



**Source:** Targeted online survey conducted by Wavestone with CAs. Q85. In your view, how could a better information sharing framework between companies be promoted? N for CAs= 46

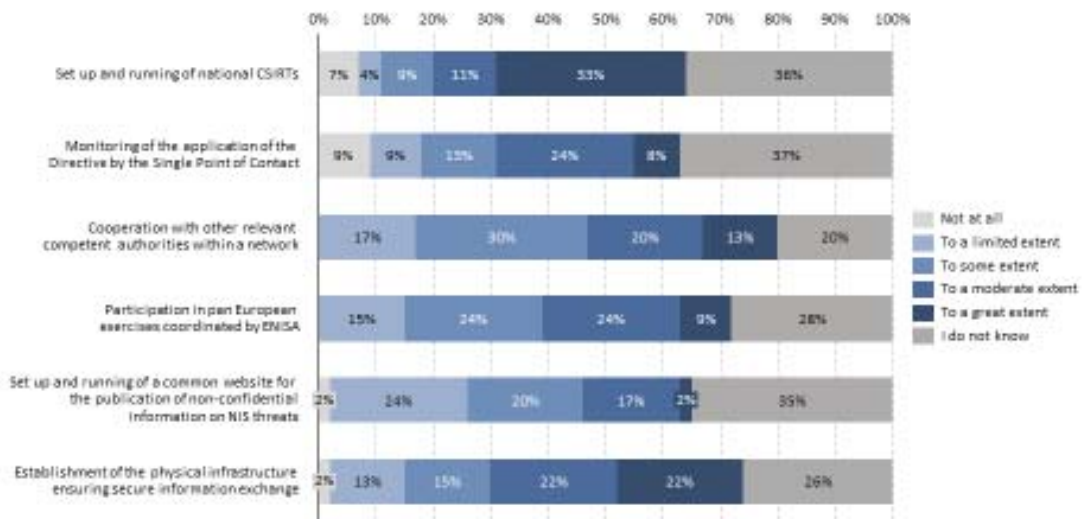
**Effectiveness: Q86.** In your opinion, and taking into account the ongoing policy initiatives on cybersecurity crises response (notably the implementation of the Blueprint Recommendation), to what extent a harmonisation at EU level of the national crisis management measures would help ensure a more effective coordinated EU response to large-scale incidents and crises?



Source: Targeted online survey conducted by Wavestone with CAs. Q86. In your opinion, and taking into account the ongoing policy initiatives on cybersecurity crises response (notably the implementation of the Blueprint Recommendation), to what extent a harmonisation at EU level of the national crisis management measures would help ensure a more effective coordinated EU response to large-scale incidents and crises? N for CAs= 46

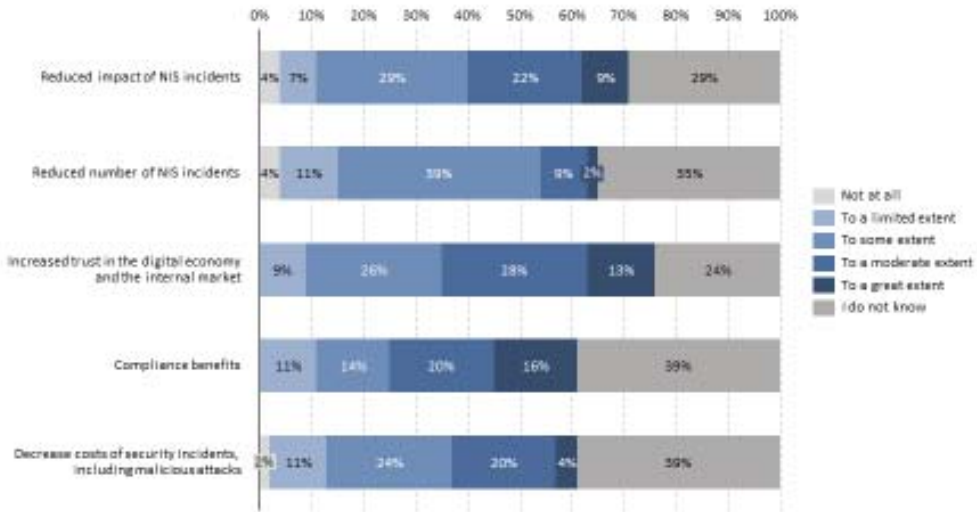
*On efficiency, compliance costs and benefits*

**Efficiency: Q87.** Considering the following compliance costs with the provisions of the NIS Directive, to what extent are they significant for the competent authorities in your country?



Source: Targeted online survey conducted by Wavestone with CAs. Q87. Considering the following compliance costs with the provisions of the NIS Directive, to what extent are they significant for the competent authorities in your country? N for CAs= 46

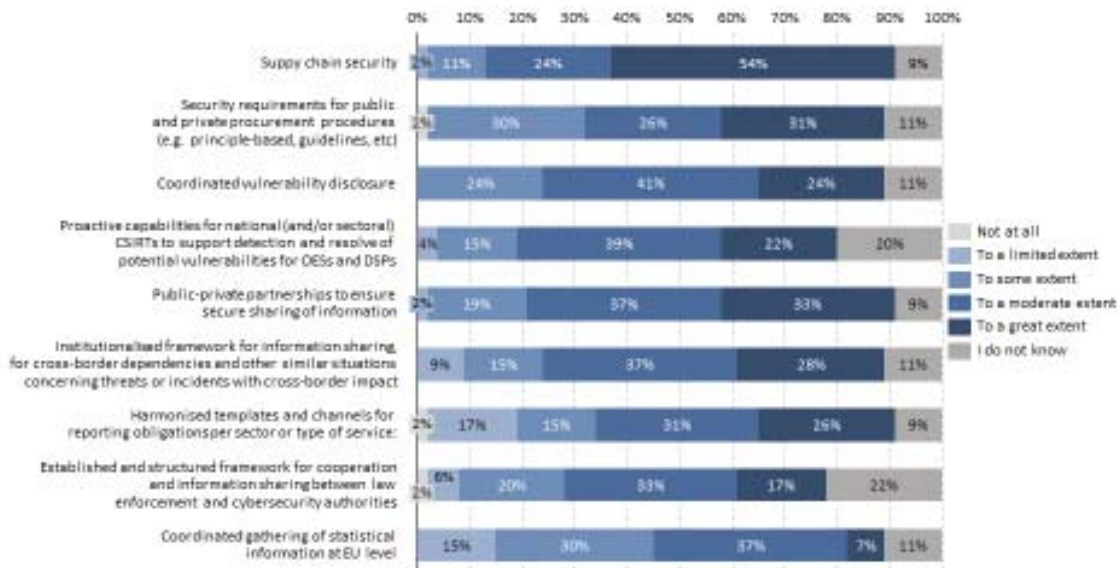
**Efficiency: Q96. Based on your experience, to what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your Case?**



Source: Targeted online survey conducted by Wavestone with CAs. Q96. Based on your experience, to what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your Case? N for CAs= 46

*On EU added value of new policy concepts*

**EU added value: Q102. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered?**

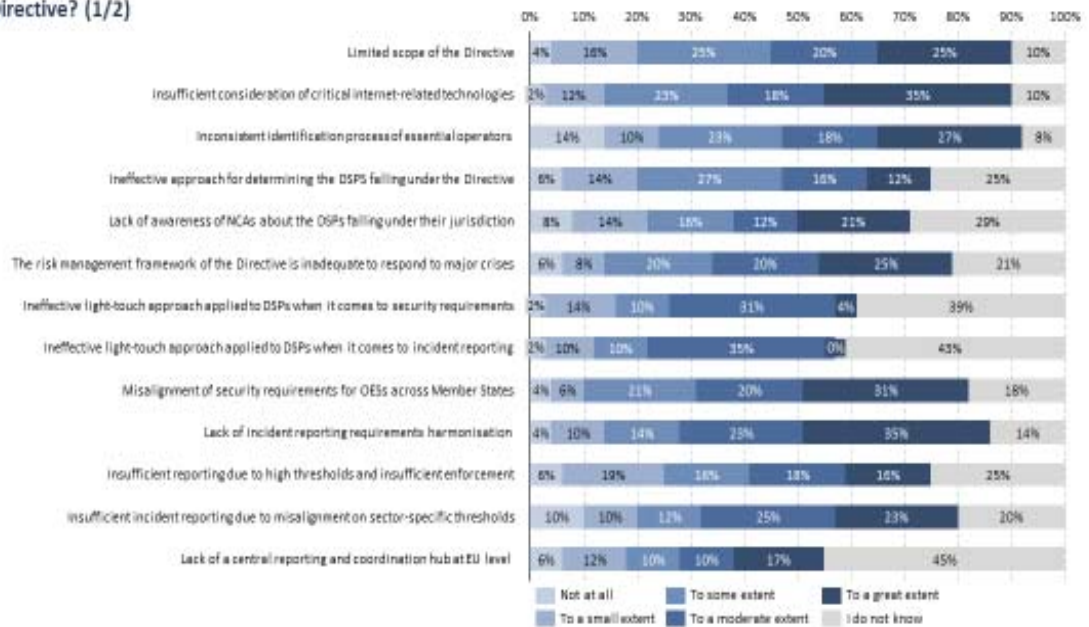


Source: Targeted online survey conducted by Wavestone with CAs. Q102. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? N for CAs= 40

**Illustrative charts on extracts from the results of the survey targeting operators of essential services**

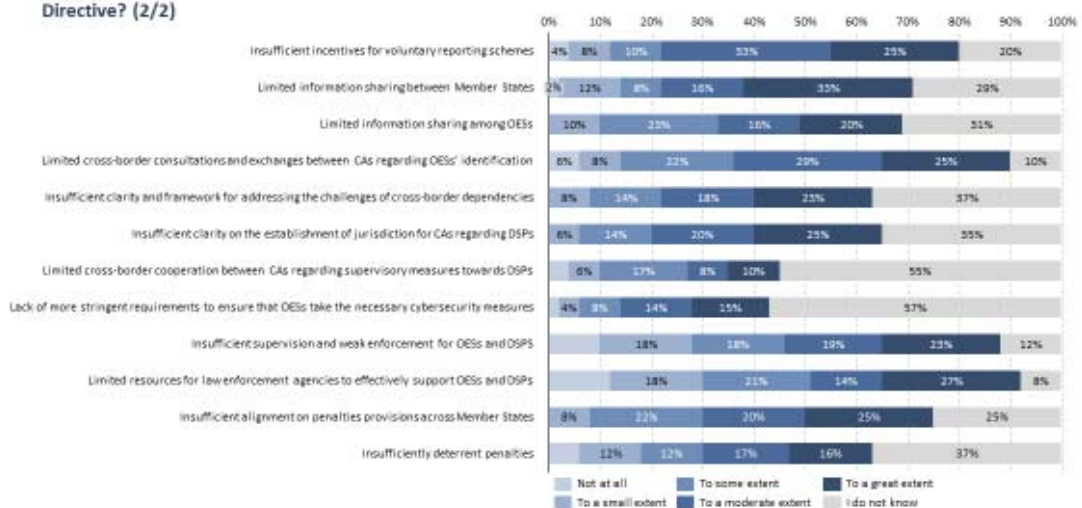
*On the shortcomings of the NIS Directive*

**Relevance: Q3. Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (1/2)**



Source: Targeted online survey conducted by Wavestone with OESs. Q3. Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for OESs=49

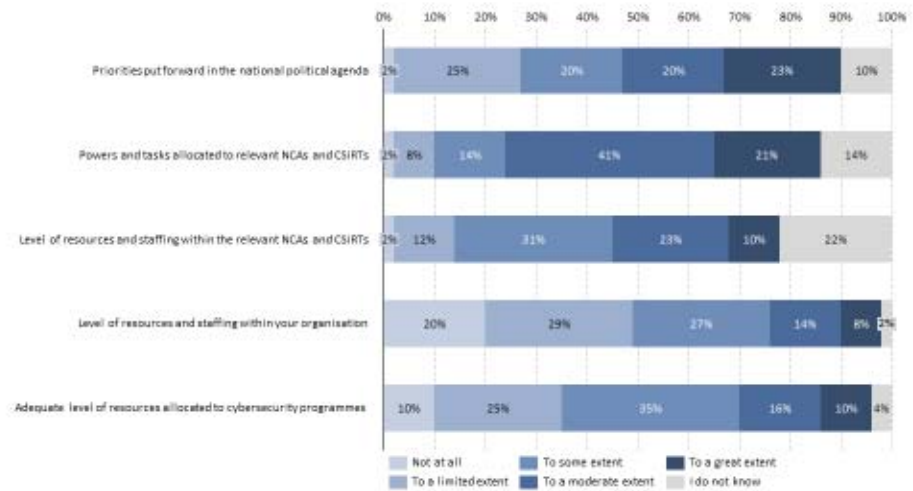
**Relevance: Q3. Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/2)**



Source: Targeted online survey conducted by Wavestone with OESs. Q3. Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for OESs=49

## On the positive effects of the NIS Directive

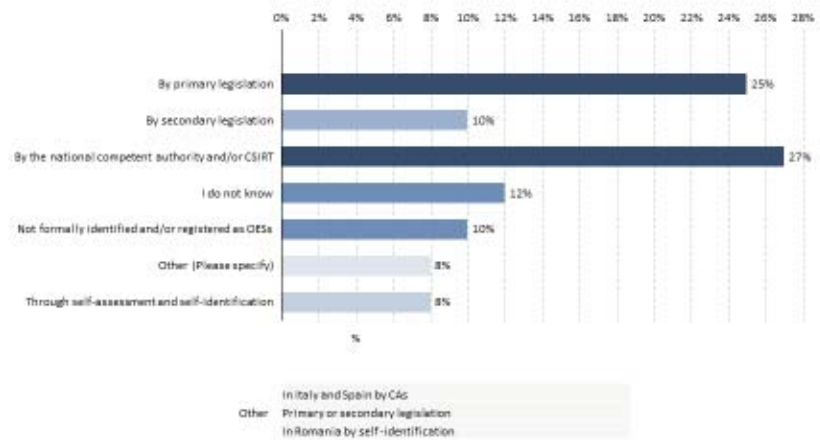
Effectiveness: Q13. To what extent has the NIS Directive positively affected the following issues in your country?



Source: Targeted online survey conducted by Weststone with OESs. Q13. To what extent has the NIS Directive positively affected the following issues in your country? N for OESs=49

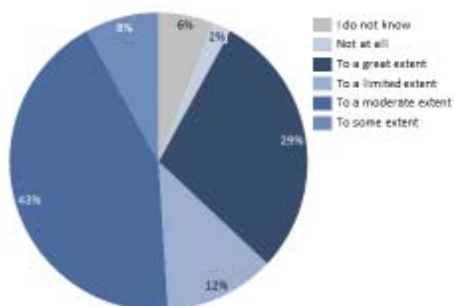
## On identification of OES

Effectiveness: Q16. How were you identified as an operator of essential services in your respective Member State?



Source: Targeted online survey conducted by Weststone with OESs. Q16. How were you identified as an operator of essential services in your respective Member State? N for OESs=49

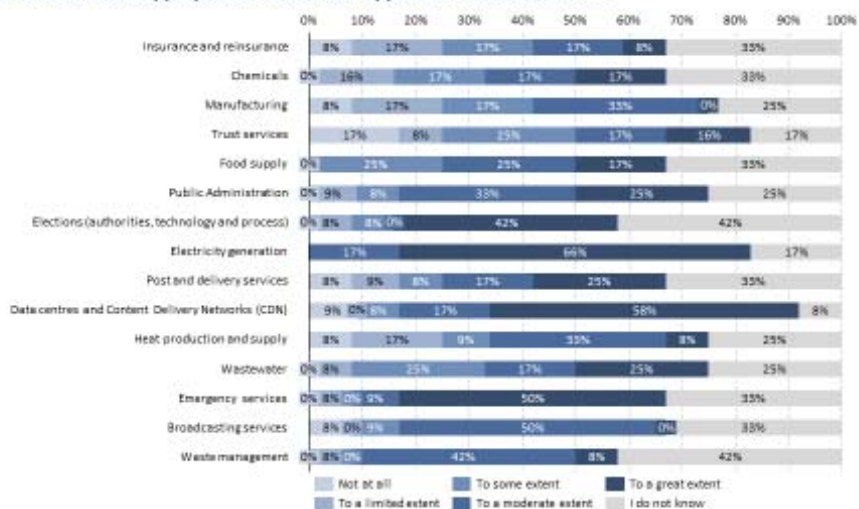
**Effectiveness: Q18.** In your opinion, to what extent are the above-mentioned criteria for the identification of operators of essential services comprehensive and/or relevant for the purpose of determining the scope of the NIS Directive?



SOURCE: Targeted online survey conducted by Wavestone with OESs. Q18. In your opinion, to what extent are the above-mentioned criteria for the identification of operators of essential services comprehensive and/or relevant for the purpose of determining the scope of the NIS Directive? N for OESs=49

### *On the scope of the NIS Directive*

**Effectiveness: Q23.** In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile? Please tick the most appropriate answer that applies for each statement.



SOURCE: Targeted online survey conducted by Wavestone with OESs. Q23. In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile? Please tick the most appropriate answer that applies for each statement. N for OESs=12



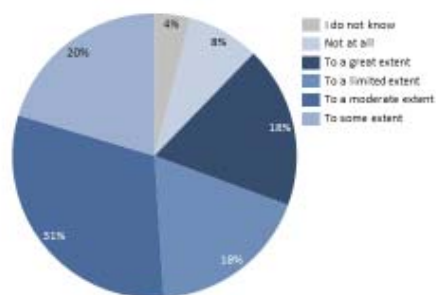
**Effectiveness: Q24.**Based on your answer to the previous question, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole? Please elaborate.



Source: Targeted online survey conducted by Wavestone with DECs. Q24.Based on your answer to the previous question, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole? Please elaborate. N for DECs=12

### *On resources*

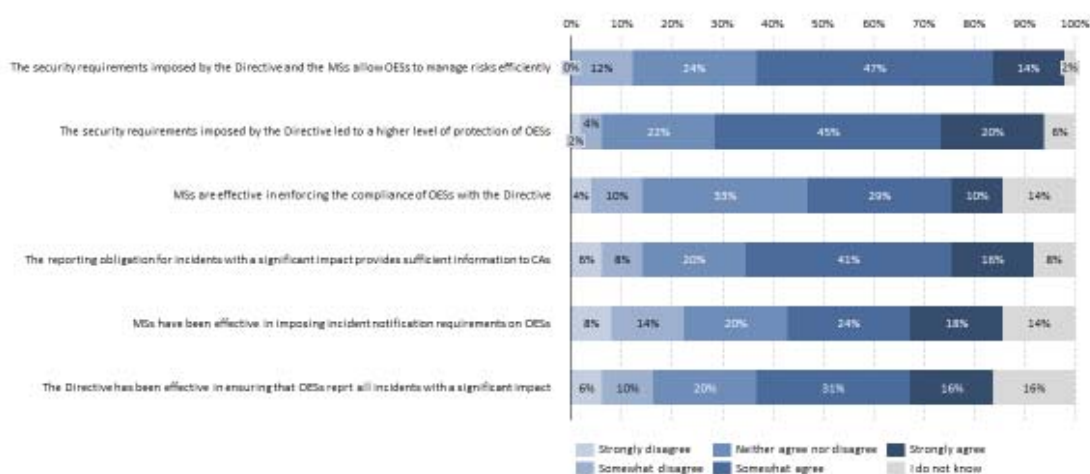
**Effectiveness: Q30.**Based on your experience, to what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate?



Source: Targeted online survey conducted by Wavestone with DECs. Q30.Based on your experience, to what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate? N for DECs=49

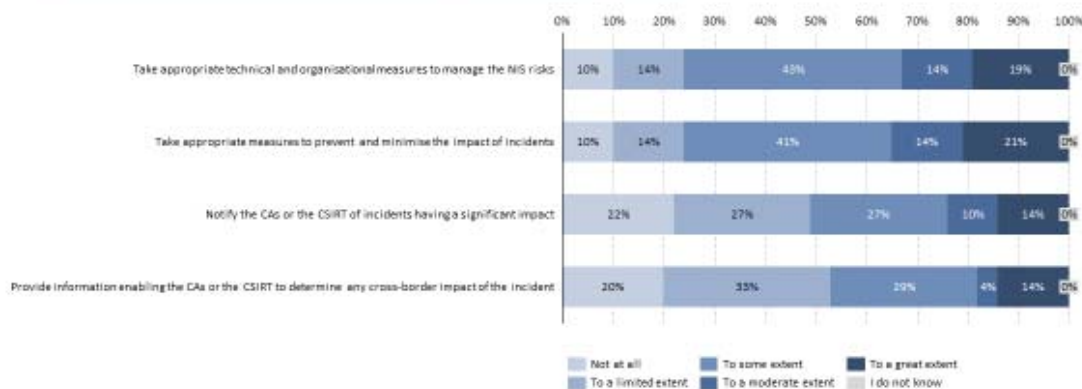
## On security requirements and incident notifications

**Effectiveness: Q32.** To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 14 of the Directive?



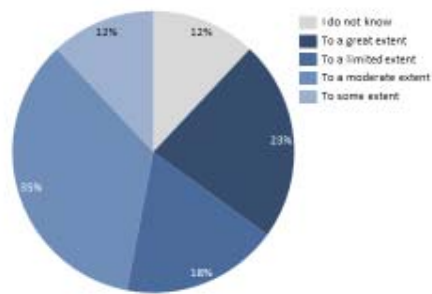
**SOURCE:** Targeted online survey conducted by Wavestone with OESs. Q32. To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 14 of the Directive? N for OESs=49

**Effectiveness: Q33.** Considering the technical and organisational requirements put forward in Article 14 of the NIS Directive to manage the risks posed to the operators of essential services' security of network and information systems used in the context of offering services referred to in Annex II within the Union, to what extent did you face challenges in the implementation of the following requirements? Considering the requirements of operators of essential services listed below, please tick the most appropriate statement.



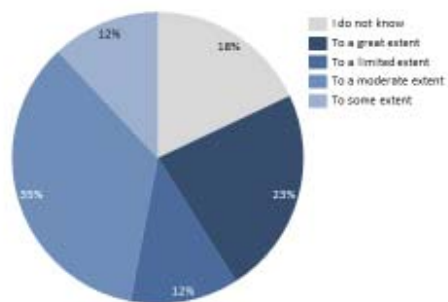
**SOURCE:** Targeted online survey conducted by Wavestone with OESs. Q33. Considering the technical and organisational requirements put forward in Article 14 of the NIS Directive to manage the risks posed to the operators of essential services' security of network and information systems used in the context of offering services referred to in Annex II within the Union, to what extent did you face challenges in the implementation of the following requirements? Considering the requirements of operators of essential services listed below, please tick the most appropriate statement. N for OESs=49

**Effectiveness: Q35.** To what extent do the requirements for security measures differ from one Member State to the other? Please reply taking account of your direct experience.



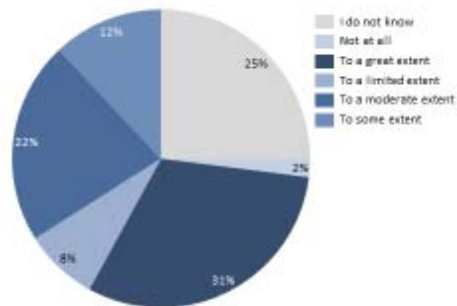
SOURCE: Targeted online survey conducted by Wavestone with OESs. Q35. To what extent do the requirements for security measures differ from one Member State to the other? Please reply taking account of your direct experience. N for OESs=49

**Effectiveness: Q37.** In your opinion, to what extent the incident notification obligations differ from one Member State to the other? Please reply taking account of your direct experience.



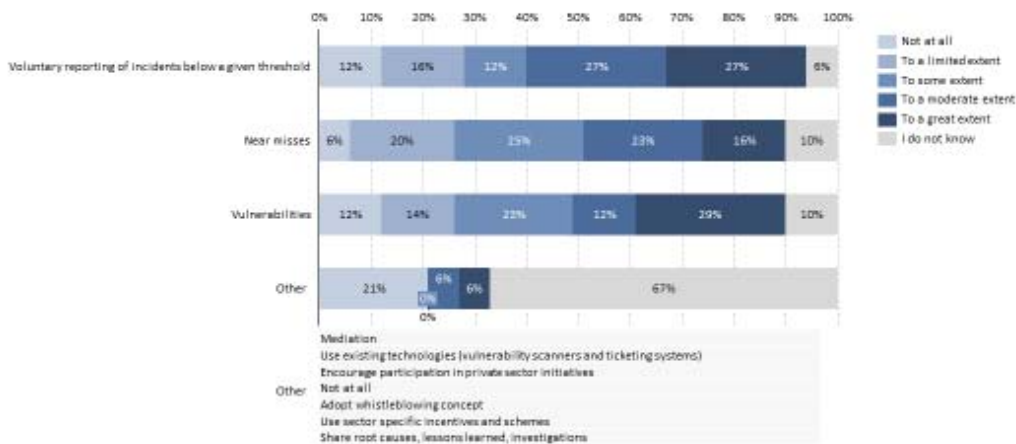
SOURCE: Targeted online survey conducted by Wavestone with OESs. Q37. In your opinion, to what extent the incident notification obligations differ from one Member State to the other? Please reply taking account of your direct experience. N for OESs=49

**Effectiveness: Q41. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension?**



**SOURCE:** Targeted online survey conducted by Wavestone with OESs. Q41. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension? N for OESs=49

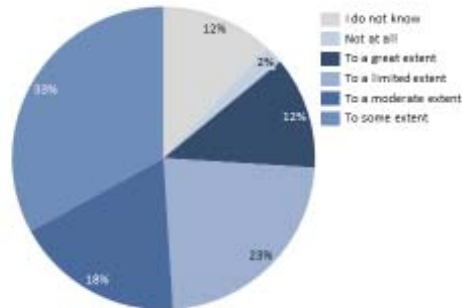
**Effectiveness: Q43. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities? Considering new ways of reporting listed below, please tick the most appropriate answer.**



**SOURCE:** Targeted online survey conducted by Wavestone with OESs. Q43. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities? Considering new ways of reporting listed below, please tick the most appropriate answer. N for OESs=49

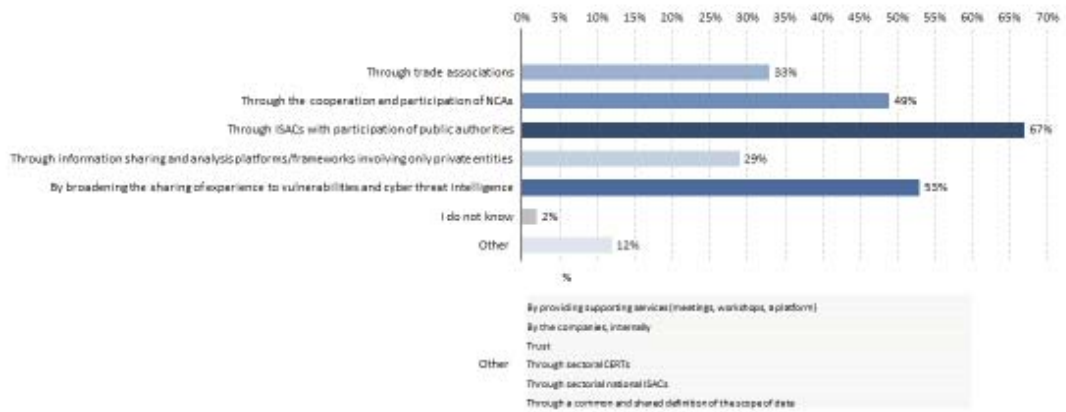
## On information sharing and cooperation

**Effectiveness: Q45. To what extent do you think the level of information sharing between public and the private sectors is effective?**



SOURCE: Targeted online survey conducted by Wavestone with DES. Q45. To what extent do you think the level of information sharing between public and the private sectors is effective? N for DES=49

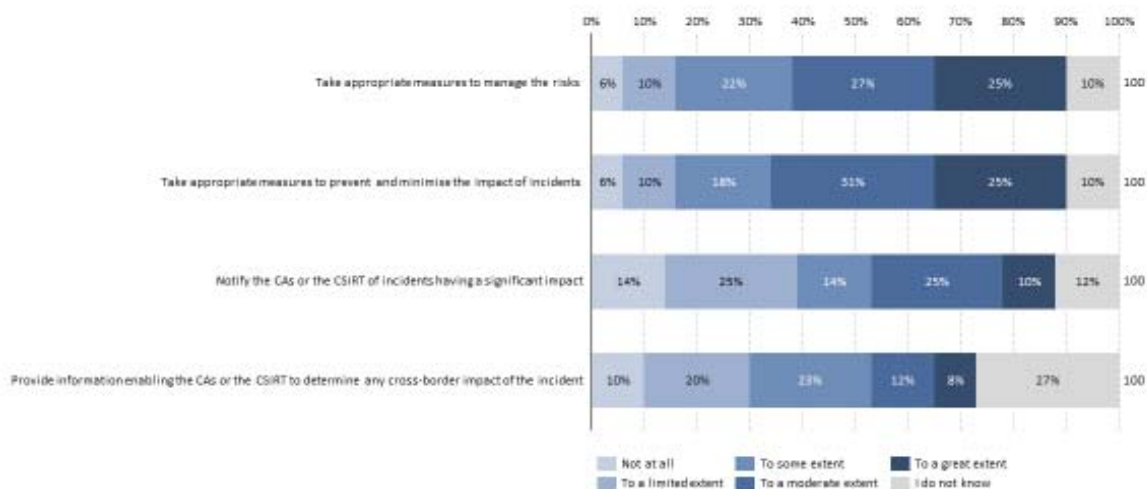
**Effectiveness: Q50. In your view, how could a better information sharing framework between companies be promoted? Please tick all that apply.**



SOURCE: Targeted online survey conducted by Wavestone with DES. Q50. In your view, how could a better information sharing framework between companies be promoted? Please tick all that apply. N for DES=49

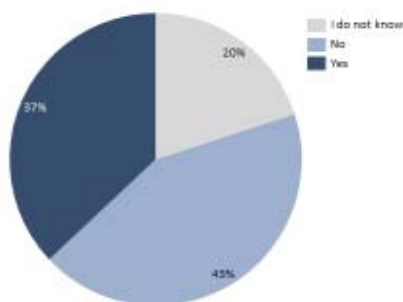
*On efficiency, compliance costs and benefits*

**Efficiency: Q51.** Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 14, to what extent were they significant for your organisation?



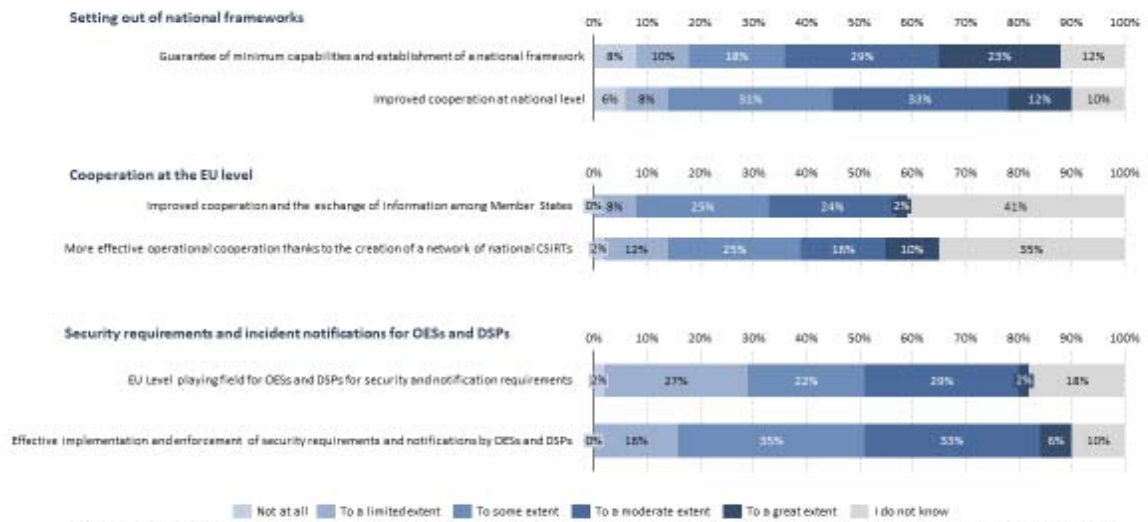
SOURCE: Targeted online survey conducted by Wavestone with DESs. Q51. Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 14, to what extent were they significant for your organisation? N for DESs=49

**Efficiency: Q52.** Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement?



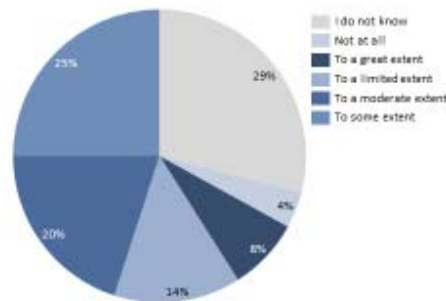
SOURCE: Targeted online survey conducted by Wavestone with DESs. Q52. Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement? N for DESs=49

**Efficiency: Q57. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case?**



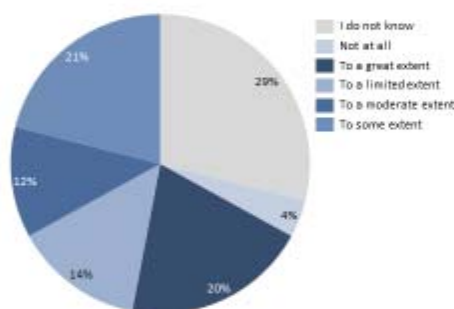
Source: Targeted online survey conducted by Wavestone with OESs. Q57. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case? N for OESs=49

**Effectiveness: Q59. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought?**



Source: Targeted online survey conducted by Wavestone with OESs. Q59. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought? N for OESs=49

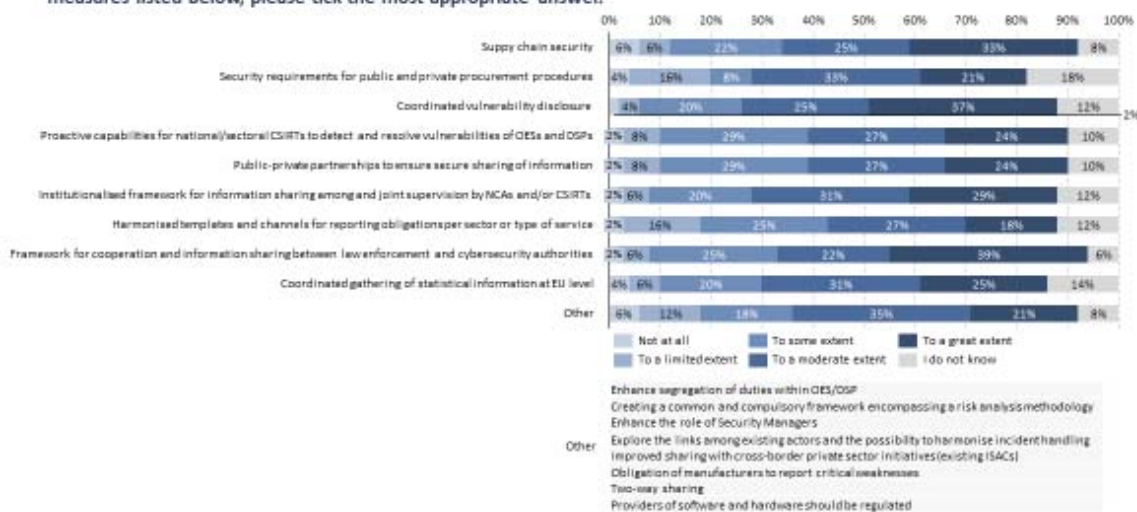
**Effectiveness: Q62.**To what extent do you think that different reporting thresholds and deadlines across the EU create unnecessary administrative burden for operators of essential services (e.g. when operating in different countries)?



**Source:** Targeted online survey conducted by Wavestone with OESs. Q62. To what extent do you think that different reporting thresholds and deadlines across the EU create unnecessary administrative burden for operators of essential services (e.g. when operating in different countries)? N for OESs=49

*On new policy concepts*

**Effectiveness: Q64.**In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? Considering the new policy measures listed below, please tick the most appropriate answer.



**Source:** Targeted online survey conducted by Wavestone with OESs. Q64. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? Considering the new policy measures listed below, please tick the most appropriate answer. N for OESs=49c



**Illustrative charts on extracts from the results of the survey targeting digital service providers**

*On shortcomings of the NIS Directive*

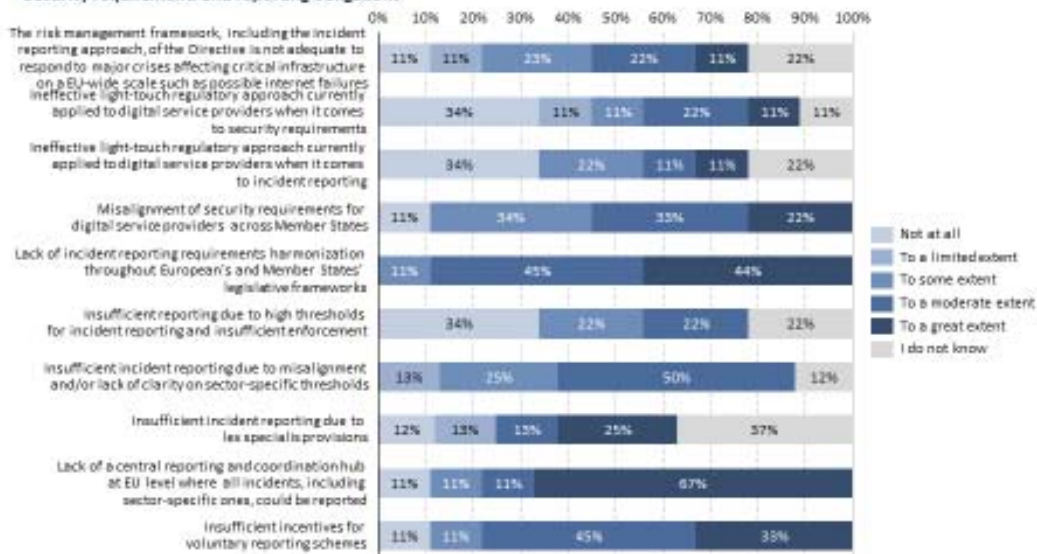
**Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (1/4)**



**Source:** Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for DSPs= 9

**Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/4)**

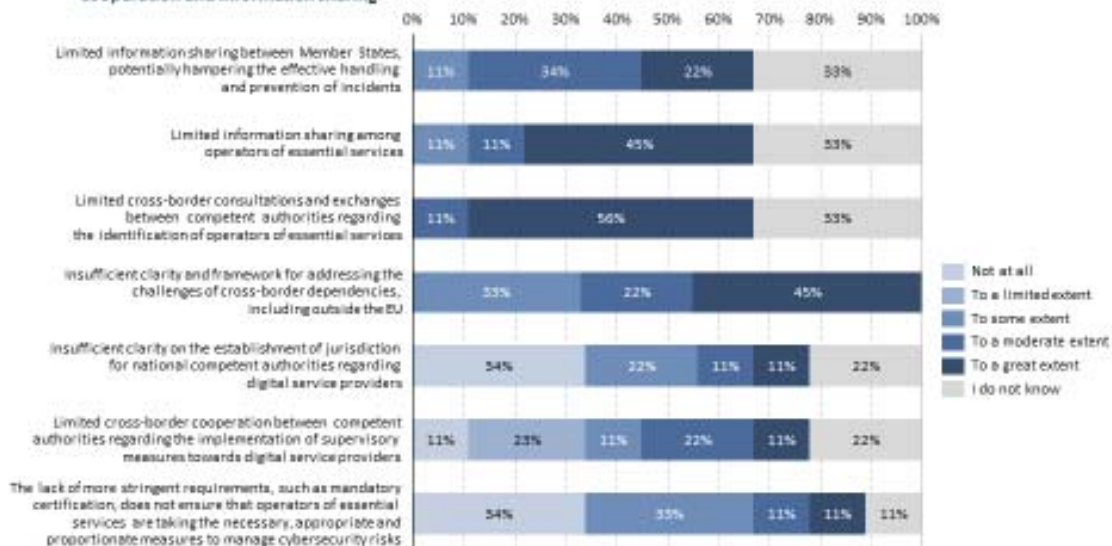
**Security requirements and reporting obligations**



Source: Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for DSPs=9

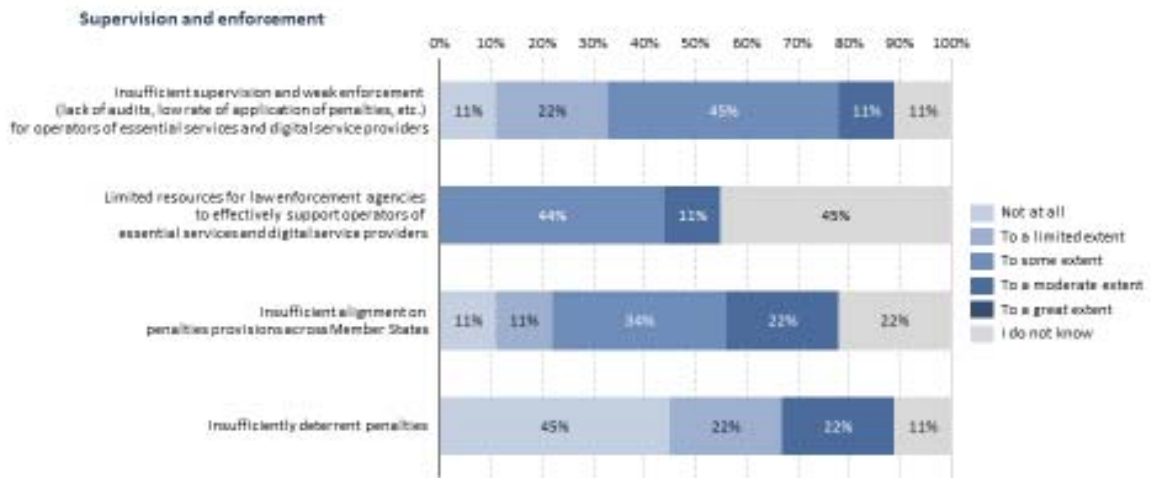
**Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (3/4)**

**Cooperation and information sharing**



Source: Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for DSPs=9

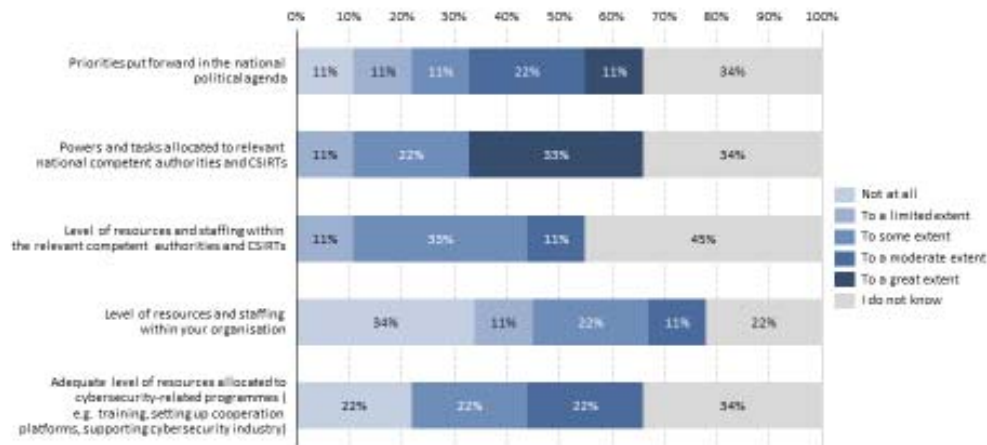
**Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (4/4)**



Source: Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for DSPs=9

*On the positive effects of the NIS Directive*

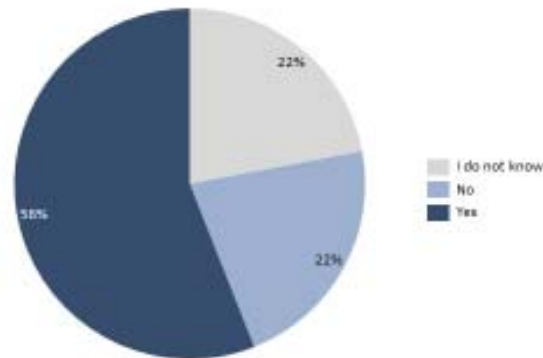
**Effectiveness: Q13. In your view, to what extent has the NIS Directive positively affected the following issues in your country?**



Source: Targeted online survey conducted by Wavestone with DSPs. Q13. In your view, to what extent has the NIS Directive positively affected the following issues in your country? N for DSPs=9

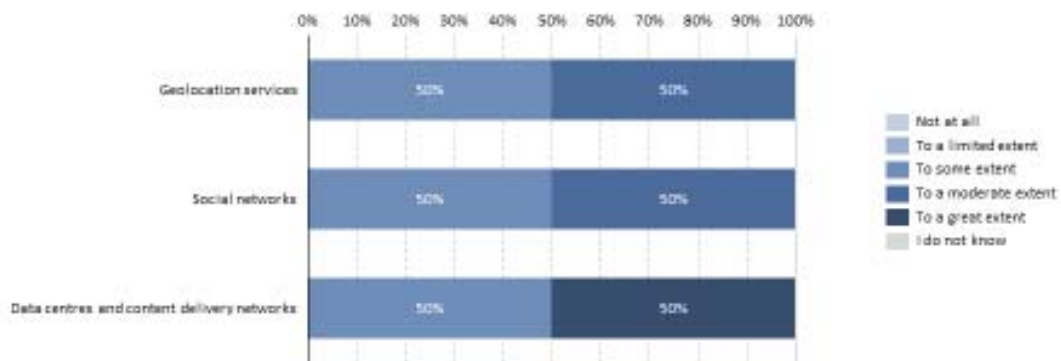
## On the scope of the NIS Directive

**Effectiveness: Q16.** In your view, does Annex III of the NIS Directive effectively cover all types of digital service providers considered as essential for the functioning of the Union's economy and society?



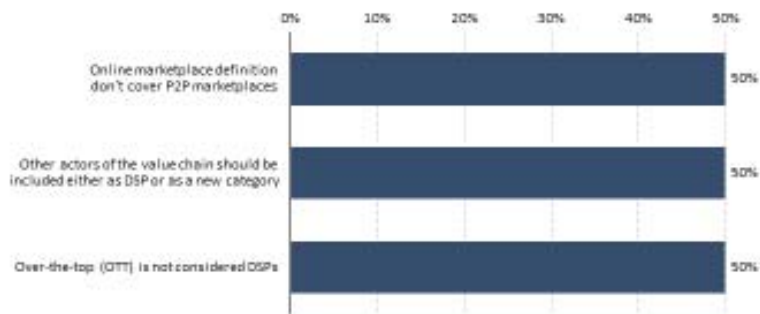
Source: Targeted online survey conducted by Wavestone with DSPs. Q16. In your view, does Annex III of the NIS Directive effectively cover all types of digital service providers considered as essential for the functioning of the Union's economy and society? N for DSPs=9

**Effectiveness: Conditional question [If "No" was answered in Q16] Q17.** In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity related risk profile?



Source: Targeted online survey conducted by Wavestone with DSPs. Conditional question [If "No" was answered in Q16] Q17. In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity related risk profile? N for DSPs= 2

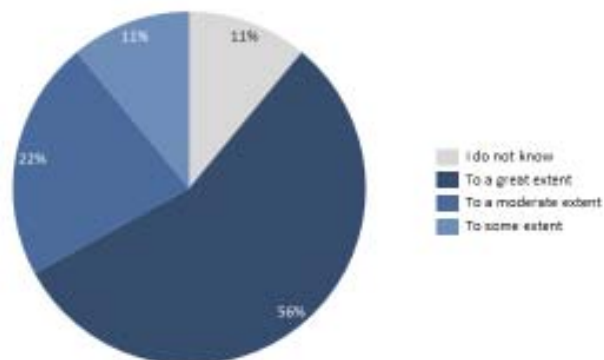
**Effectiveness: Conditional question [If "No" was answered in Q16] Q18. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union's economy and society?**



SOURCE: Targeted online survey conducted by Wavestone with DSPs. [If "No" was answered in Q16] Q18. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union's economy and society? N for DSPs= 2

*On resources*

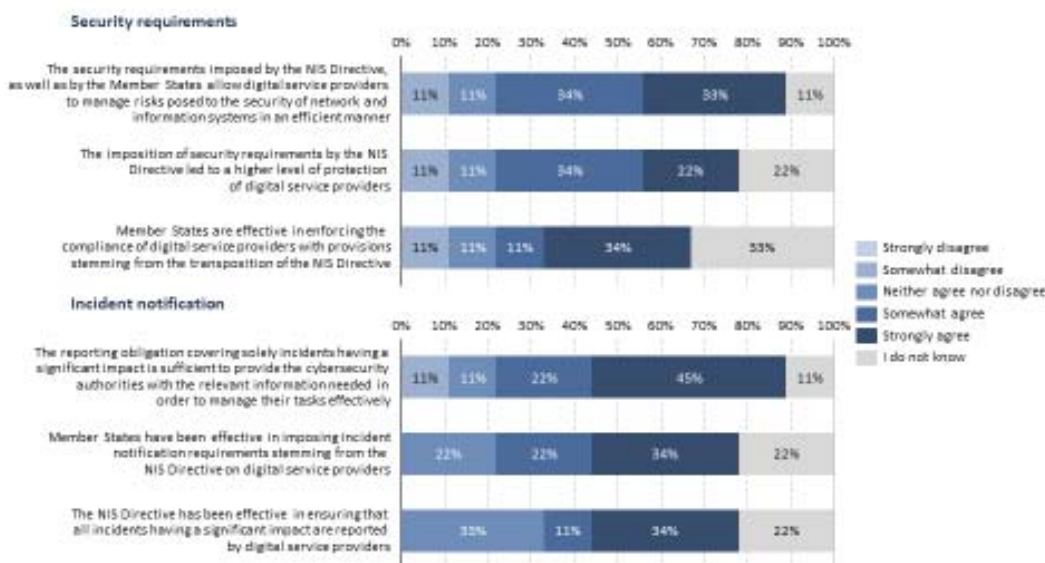
**Effectiveness: Q26. To what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate?**



SOURCE: Targeted online survey conducted by Wavestone with DSPs. Q26. To what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate? N for DSPs= 9

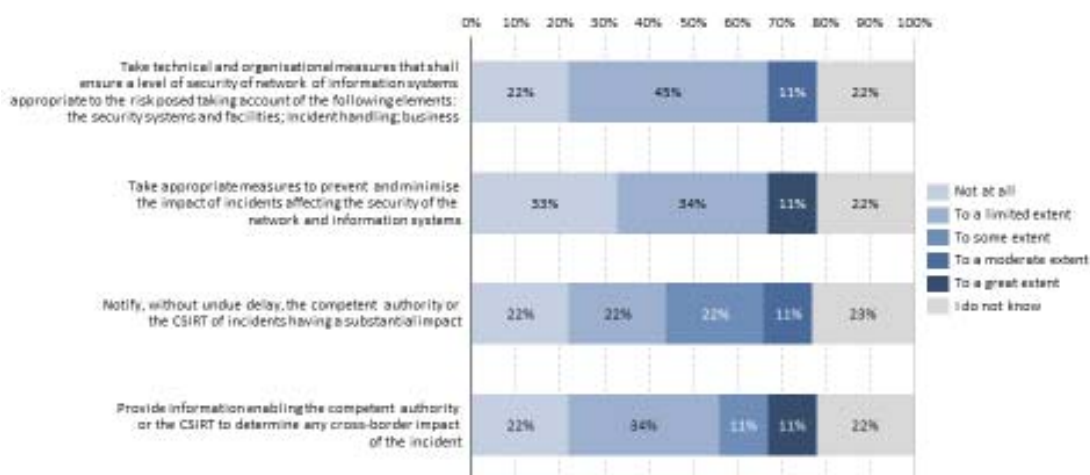
## On security requirements and incident notifications

### Effectiveness: Q28. To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 16 of the Directive?



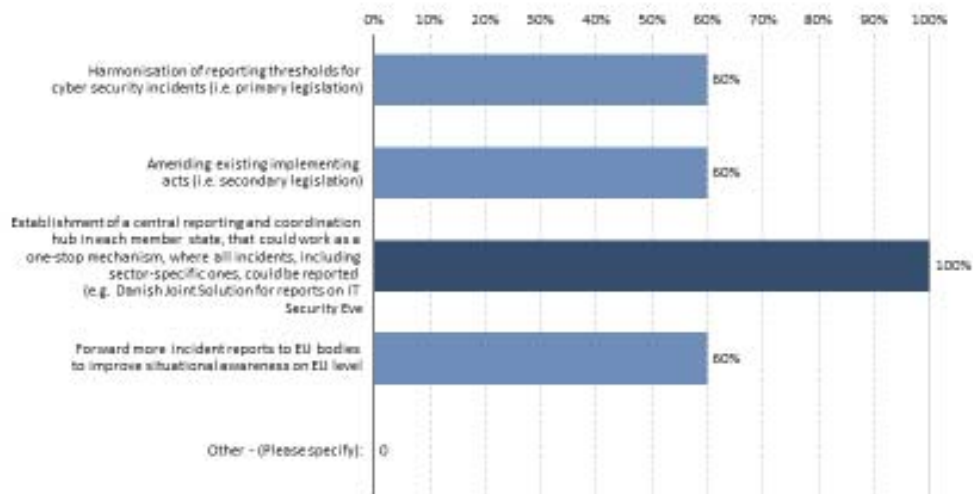
Source: Targeted online survey conducted by Wavestone with DSPs. Q28. To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 16 of the Directive? N for DSPs= 9

### Effectiveness: Q29. Considering the technical and organisational requirements put forward in Article 16 of the NIS Directive to manage the risks posed to the digital service providers' security of network and information systems used in the context of offering services referred to in Annex III within the Union, to what extent did you face challenges in the implementation of the following requirements?



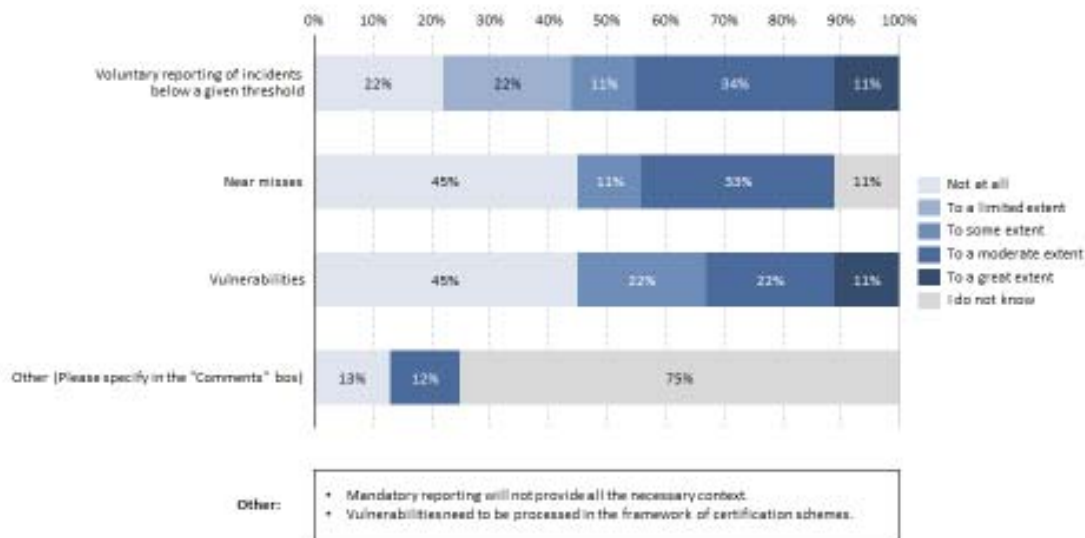
Source: Targeted online survey conducted by Wavestone with DSPs. Q29. Considering the technical and organisational requirements put forward in Article 16 of the NIS Directive to manage the risks posed to the digital service providers' security of network and information systems used in the context of offering services referred to in Annex III within the Union, to what extent did you face challenges in the implementation of the following requirements? N for DSPs= 9

**Effectiveness: Conditional question [If "To a moderate extent", "To a great extent" was answered in Q37] Q38. Which of the below options should be considered as means to further streamline the incident notification process?**



**Source:** Targeted online survey conducted by Wavestone with DSPs. Conditional question [If "To a moderate extent", "To a great extent" was answered in Q37] Q38. Which of the below options should be considered as means to further streamline the incident notification process? N for DSPs= 5

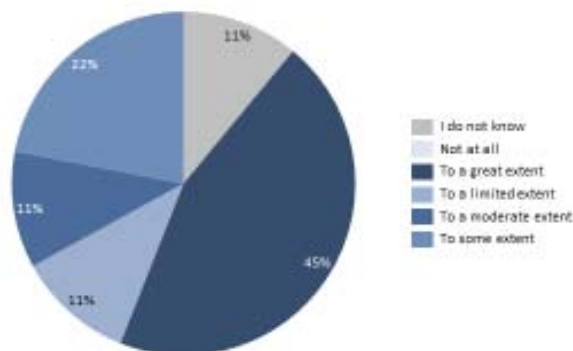
**Effectiveness: Q39. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities?**



**Source:** Targeted online survey conducted by Wavestone with DSPs. Q39. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities? N for DSPs= 9

## On the light-touch approach for supervision

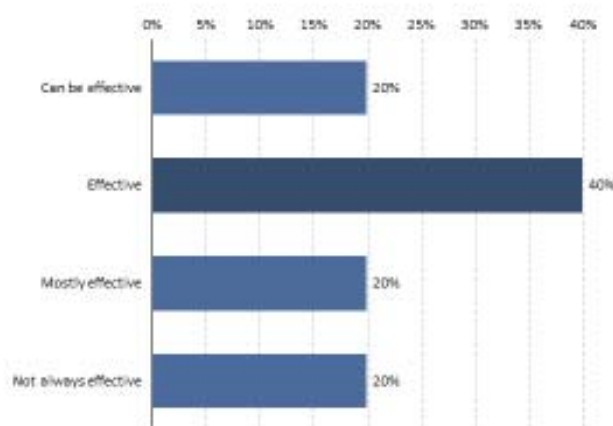
**Effectiveness: Q40. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital service providers effective?**



SOURCE: Targeted online survey conducted by Wavestone with DSPs. Q40. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital service providers effective? N for DSPs= 9

## On information sharing and cooperation

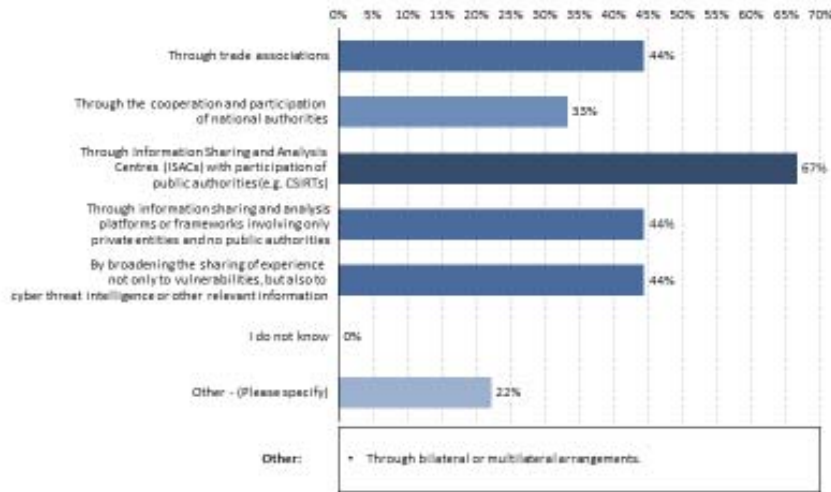
**Effectiveness: Conditional question : [If "Digital service provider within your sector", "Digital service provider from other sectors in the same Member State", "Digital service provider from the same sector from another Member State", "Operators of essential service in the same Member State", "Operator of essential service from another Member State", "Other - (Please specify)" was answered in Q44] Q46. Could you please specify whether you consider this information sharing with other private entities effective?**



SOURCE: Targeted online survey conducted by Wavestone with DSPs. Conditional question : [If "Digital service provider within your sector", "Digital service provider from other sectors in the same Member State", "Digital service provider from the same sector from another Member State", "Operators of essential service in the same Member State", "Operator of essential service from another Member State", "Other - (Please specify)" was answered in Q44] Q46. Could you please specify whether you consider this information sharing with other private entities effective? N for DSPs= 5



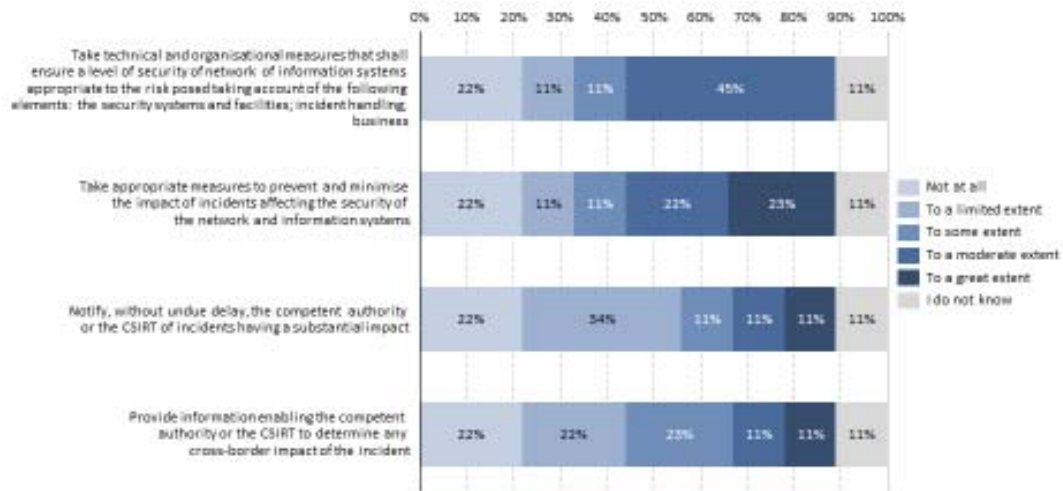
**Effectiveness: Q47. In your view, how could a better information sharing framework between companies be promoted?**



**SOURCE:** Targeted online survey conducted by Wavestone with DSPs. Q47. In your view, how could a better information sharing framework between companies be promoted? N for DSPs= 9

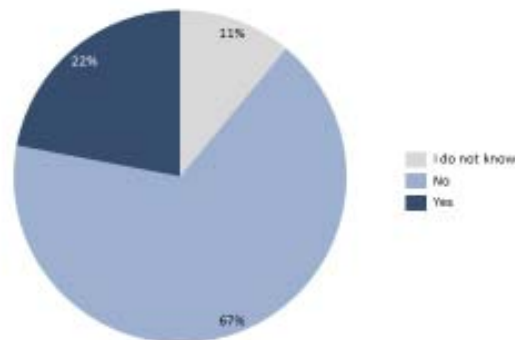
*On efficiency, compliance costs and benefits*

**Efficiency: Q48. Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 16, to what extent were they significant for your organisation?**



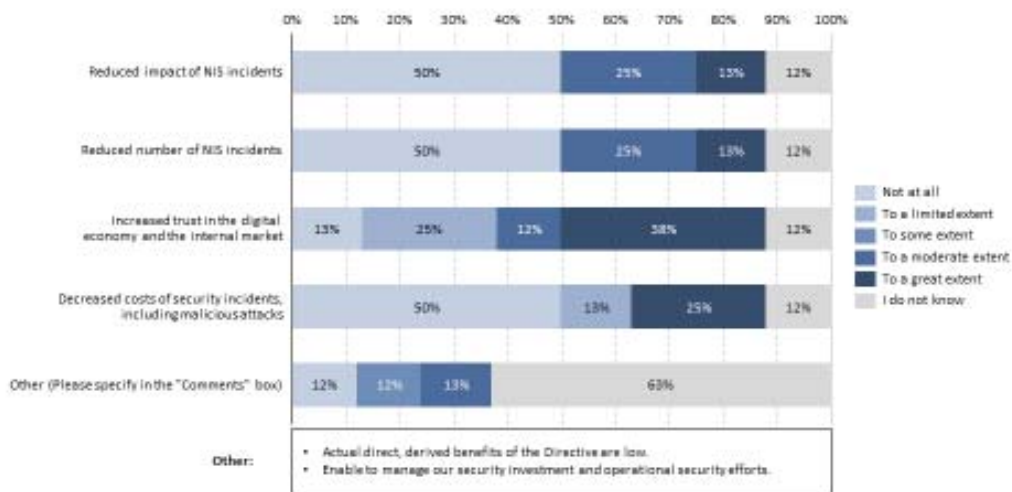
**SOURCE:** Targeted online survey conducted by Wavestone with DSPs. Q48. Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 16, to what extent were they significant for your organisation? N for DSPs= 9

**Efficiency: Q49. Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement?**



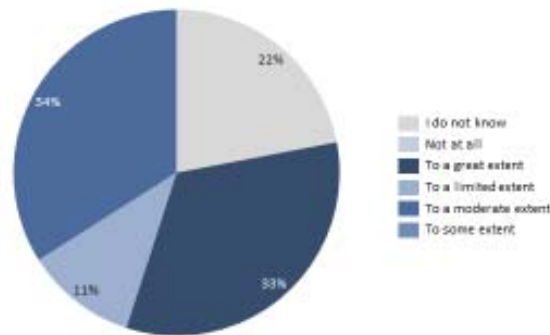
**Source:** Targeted online survey conducted by Wavestone with DSPs. Q49. Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement? N for DSPs= 0

**Efficiency: Q54. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case?**



**Source:** Targeted online survey conducted by Wavestone with DSPs. Q54. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case? N for DSPs= 8

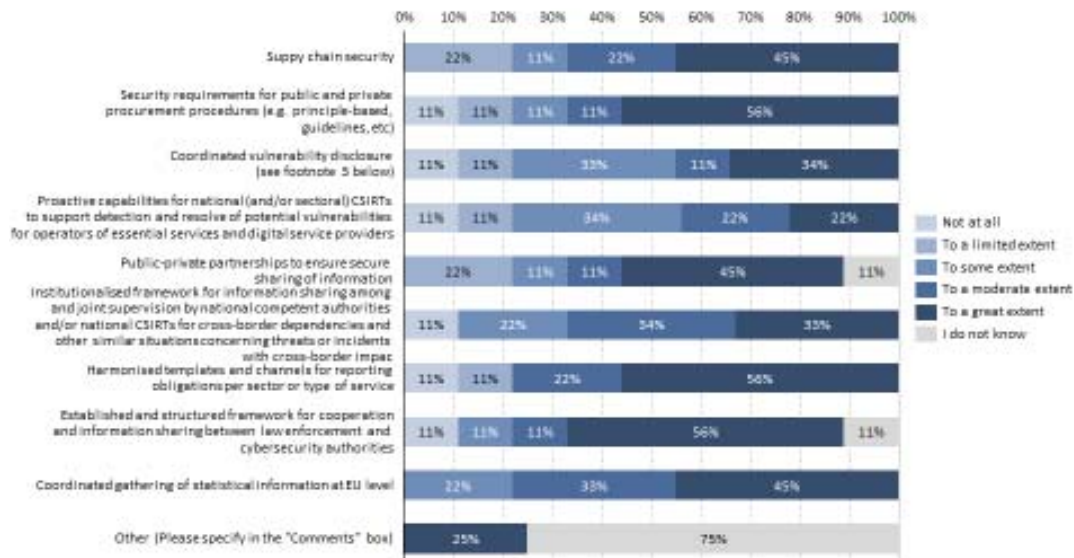
**Efficiency: Q56. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought?**



Source: Targeted online survey conducted by Wavestone with DSPs. Q56. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought? N for DSPs= 9.

*On new policy concepts*

**Added value: Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? (1/2)**



Source: Targeted online survey conducted by Wavestone with DSPs. Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? N for DSPs= 9.

Added value: Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? (2/2)

Other:

- Coordinated vulnerability disclosures: carefully evaluate potential additions.
- EU authority for cybersecurity incident reporting: include other subject in review process.
- Harmonization between legislations.
- Industry cooperation in NIS cooperation Group and CSIRTs Network. Recognizing that the NIS Directive supports public private cooperation (example, an annual public private meeting or Industry Stakeholder Group).
- Information sharing framework between companies: worked with competent authorities.
- IoT security baseline.
- Legal basis for cybersecurity processing operations.
- Managing different maturity levels.
- More formally define what a "User" is in the cloud context.
- Reviewing key definitions and identifying and addressing.
- Role of CISO.

Source: Targeted online survey conducted by Wavestone with DSPs. Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? N for DSPs: 9

## ANNEX 7: OVERVIEW OF RELATED CYBERSECURITY LEGAL ACTS AND POLICY MEASURES

The EU Cybersecurity Act<sup>1</sup> entered into force in June 2019, including provisions that (i) equip Europe with a framework of cybersecurity certification of products, services and processes, making sure that connected devices are reliable and trustworthy, and (ii) reinforce the mandate of the EU Agency for Cybersecurity (ENISA) to better support Member States with tackling cybersecurity threats and attacks. One of the main aims of the Cybersecurity Act is to develop a **culture of cybersecurity by design**, with security built into products and services from the start. The new cybersecurity certification framework under the Cybersecurity Act is now being implemented, with two certification schemes already in preparation, and priorities for further schemes to be identified in the Union Rolling Work Programme on cybersecurity certification.<sup>2</sup>

Further EU legislative and policy measures relevant to cybersecurity are also being taken in connected areas. The Commission is currently preparing a proposal, due by the end of 2020, for additional measures to enhance the protection and resilience of critical infrastructure. The Directive on the identification and designation of **European critical infrastructures**<sup>3</sup> (hereinafter called ‘the ECI Directive’) established a process to identify, designate and adopt protection measures for infrastructures that are critical from a European perspective, i.e. where their disruption would have an impact on at least two Member States, limited to the transport and energy sectors.<sup>4</sup> While the NIS Directive aims at ensuring that operators in the seven sectors it covers take appropriate and proportionate technical and organisational measures to manage the cybersecurity risks that their network and information systems are exposed to, irrespective of the extent of their operations over national borders, or the cross-border implications in the event of disruptions, the ECI Directive aims to enhance the general, largely physical protective arrangements surrounding designated infrastructures of cross-border significance in the energy and transport sectors alone. In 2019, the Commission conducted an evaluation of the ECI Directive, concluding that it is only of partial relevance today, in light of a range of factors including considerable changes in the context in which critical infrastructure operates in. The stated objectives of the initiative are to ensure greater coherence of the EU critical infrastructure protection approach, to include all relevant sectors providing essential services, including those defined by the NIS framework, to help Member States to achieve resilience of national infrastructures and to improve information exchange and cooperation.

Overall, since the implementation of the NIS Directive, European countries have become increasingly dependent on digital and information systems, while their networks have become ever-more interconnected. Within the Commission Work Programme 2020<sup>5</sup>, cybersecurity is presented as being interlinked with the digitalisation of the European

---

<sup>1</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1.

<sup>2</sup> <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/>

<sup>3</sup> Directive 2008/114/EC of 8 December 2008

<sup>4</sup> The 2006 proposal for the ECI Directive (COM(2006) 787) identified a total of 11 critical infrastructure sectors, including: energy; nuclear industry; information, communication technologies, ICT; water; food; health; financial; transport; chemical industry; space; and research facilities.

<sup>5</sup> COM (EU) (2020) 37 final, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Commission Work Programme 2020, 29.1.2020.

Union. Technologies used in critical sectors such as healthcare, energy, banking, and legal systems will have to be reinforced by the development of robust cybersecurity measures. Consequently, a number of other **sector-specific** legal acts or upcoming legislative proposals are also addressing cybersecurity-related aspects, as follows:

- as regards the *financial sector*, the Commission launched an initiative for a Digital Operational Resilience Framework for financial services, adopted on 24 September 2020<sup>6</sup>. The initiative is *lex specialis* in relation with the NIS Directive, setting out consolidated, simplified and upgraded ICT risk requirements throughout the financial sector to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks for their operations.
- in the *energy sector*, the Risk Preparedness Regulation<sup>7</sup> inter alia sets a framework to ensure that Member States prevent and manage crisis situations in cooperation with each other in a spirit of solidarity. This Regulation complements the NIS Directive “by ensuring that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans”.<sup>8</sup> The same applies to the Regulation<sup>9</sup> concerning measures to safeguard the security of gas. Both instruments are accompanied by a Commission Recommendation<sup>10</sup> on cybersecurity in the energy sector providing sector-specific guidance. Furthermore, as part of the development of network codes and guidelines for the period 2020-2023 for electricity and for 2020 for gas, a Network Code for the cybersecurity of cross-border energy flows is being established<sup>11</sup>. In this context, sector-specific rules for cyber security aspects of cross-border electricity flows should allow the electricity networks to address potential cyber threats so that clean energy is fit for the digital age
- in the *transport sector*, additional initiatives are being put forward by the Commission and relevant EU bodies, with the aim of increasing the robustness of services against cyberattacks. Such initiatives regard, for example, the *aviation sector*, where, the EU adopted detailed rules for cybersecurity in the aviation security domain<sup>12</sup>. The EU Aviation Safety Agency (EASA) is preparing an opinion to be submitted to the European Commission in order to amend aviation safety legislation with cybersecurity provisions requiring the mandatory introduction of an Information Security Management System. In *maritime transport*, EU security legislation<sup>13</sup> already contains provisions relating to cybersecurity. Cybersecurity is also part of the EU Maritime Security Strategy dating from 2014<sup>14</sup>, with an action plan revised in 2018. In addition, the

---

<sup>6</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020) 595 final.

<sup>7</sup> Regulation (EU) 2019/941.

<sup>8</sup> Recital 7 of Regulation (EU) 2019/941 (Risk Preparedness Regulation).

<sup>9</sup> Regulation (EU) 2017/1938.

<sup>10</sup> C(2019)2400 final of 3 April 2019.

<sup>11</sup> As empowered by Regulation (EU) 2019/943 on the internal market for electricity. Preparatory work was finalised in September 2019, an informal drafting process is ongoing,

<sup>12</sup> Commission Implementing Regulation (EU) 2019/1583

<sup>13</sup> Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

<sup>14</sup> <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT>

Commission, the EU Aviation Safety Agency (EASA), the European Maritime Safety Agency (EMSA) and ENISA rely on a series of expert groups gathering representatives from the different modes of transport to exchange viewpoints and ideas on cyber security threats, challenges and solutions. For example, cybersecurity is regularly discussed between the Commission, Member States and stakeholders at the level of transport security committee meetings for each mode<sup>15</sup>. EASA chairs a European Strategic Coordination Platform (ESCP) including key industry stakeholders, Member States and EU Institutions. This has led to the first common EU strategy for cybersecurity in aviation. It is also supporting the creation of a European Centre for Cybersecurity in Aviation (ECCSA) and providing the initial operational capabilities currently in collaboration with CERT-EU. With the support of ENISA, the Transport Resilience and Security Expert Group (TRANSSEC) was also set up, gathering experts from the transport sector to exchange viewpoints and ideas on cyber security threats, challenges and solutions.

As regards *electronic communication networks and services*, the cybersecurity aspects in relation to these are now regulated, starting 21 December 2020, by the European Electronic Communications Code (EECC). The NIS Directive excludes from its security and notification requirements undertakings providing public communications networks or publicly available electronic communications services, which are subject to the requirements of Articles 13a and 13b of Framework Directive 2002/21/EC, which is repealed with effect from 21 December 2020.<sup>16</sup> The Connectivity Package, which reshapes telecoms regulation, redefines the term ‘electronic communications network’ in the EECC. A so-called ‘Article 13a group’ made of Member States representatives and supported by ENISA, distinct from the Cooperation Group, is covering the cybersecurity policy aspects related to electronic communication networks and services and would continue to do so absent any changes to the NIS Directive. Seven Member States added the **electronic communication networks and services** to the scope of the NIS-related rules.

*The table below developed by the NIS review study points to the specific provisions of the NIS Directive and other EU legislation that are inter-related, notably as regard the security requirements and reporting obligations.*

---

<sup>16</sup> The Connectivity Package, which reshapes telecoms regulation, redefines the term ‘electronic communications network’ in the EECC.

## NIS Directive - External coherence with other EU interventions

### European Electronic Communications Code (EECC)

Provisions	NIS Directive	EECC Directive	Analysis
<b>Security notification requirements</b>	<b>Article 14(1) NIS Directive:</b> requires Member States to ensure that the OES <i>'take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.'</i>	<b>Article 40 EECC:</b> requires Member States to ensure that providers of electronic communications networks or of publicly available electronic communications services <i>'take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and systems.'</i>	Both provisions take a <b>risk-based approach</b> when implementing security measures. While the <b>NIS Directive</b> refers to <i>'security of network and information systems'</i> , <b>the EECC</b> refers to <i>'security of networks and services'</i> with both defining security as <i>'the ability of'</i> network and information systems/electronic communications networks and services <i>'to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality'</i> of stored or transmitted or processed data/of those networks and services.



## NIS Directive - External coherence with other EU interventions

	<p><i>Article 14(3) NIS Directive require Member States to ensure that security incidents having a significant impact on the continuity of the essential services/on the operation of networks or services, are reported without undue delay.</i></p>	<p><i>Article 40(2) EECC require Member States as well to ensure that security incidents having a significant impact on the continuity of the essential services/on the operation of networks or services, are reported without undue delay.</i></p>	<p><i>Overall, no divergences between the framework on security measures in the NIS Directive and EECC could be identified. However, as a mere formality, there should be alignment as regards the notion of 'incident' in the NIS Directive and 'security incidents' in the EECC, although the definitions are similar.</i></p> <p><i>In addition, there could be a potential coherence issue for reporting schemes related to Internet Service Providers (ISPs) between Article 14 NIS Directive and Article 40 EECC if the new reporting scheme implemented under Article 40 EECC was not followed: one incident could be reported under two different requirements.</i></p>
--	---	--	---

<b>Electronic identification and trust services for electronic transactions (eIDAS Regulation)</b>			
<b>Provision</b>	<b>NIS Directive</b>	<b>eIDAS Regulation</b>	<b>Analysis</b>
<b>Security notification requirements</b>	<i>Article 1(3) of the NIS Directive, require that the security and notification requirements provided for in the NIS Directive shall not apply to trust service providers which are subject to the requirements of Article 19 eIDAS Regulation.</i>	<i>Articles 19(1) and 19(2) eIDAS Regulation require inter alia that providers of trust services take appropriate security measures to mitigate risks posed to the security of their trust services and notify, without undue delay but in any event within 24 hours after becoming aware of it, the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that ‘has a significant impact on the trust service provided or on the personal data maintained therein’.</i>	<i>Coherence issues may arise when digital certificates are used for authentication in services that fall under the scope of the NIS Directive. This is likely with regard to financial services or cloud services. In addition, under the eIDAS Regulation the reporting time frame is 24 hours, whereas NIS Directive requires it to happen ‘without undue delay’.</i>

<b>General Data Protection Regulation (GDPR)</b>			
<b>Provision</b>	<b>NIS Directive</b>	<b>GDPR Regulation</b>	<b>Analysis</b>
<b>Security notification requirements</b>	Articles 8(6) and 15(4) NIS Directive require the competent authorities and single point of contact under the NIS Directive to consult and cooperate with national data protection authorities	Article 33(1) GDPR require data controllers to notify a personal data breach to the supervisory authority without undue delay, at the latest within 72 hours after becoming aware of it. In addition, if the data breach is likely to result in a high risk to the rights and freedoms of natural persons and non of the conditions described in Article 33(3) applies, controllers are required to communicate the personal data breach to the data subject without undue delay.	The difference to the NIS Directive is that the GDPR is only applicable to <b>incidents that concern personal data</b> and upon the condition that the data breach results to a risk to the rights and freedoms of natural persons. Even if one may, in theory, distinguish between incidents falling under the GDPR and such falling under the NIS Directive, in practice, <b>most security incidents will involve (at least potentially) some personal data.</b> However since the legal instruments have different objectives legal instruments. This means that OESs and DSPs will have to <b>report</b> as subset of security incidents <b>to both competent authorities</b> in order to ensure compliance with both regulatory requirements.

<i>Payment services in the internal market (PSD2 Directive)</i>			
<b>Provision</b>	<i>NIS Directive</i>	<i>PSD2 Directive</i>	<i>Analysis</i>
<b>Security notification requirements</b>	<i>Article 14(5) NIS Directive requires the competent authority to notify the relevant authorities in other Member States if the incident is of relevance for them.</i>	<p><i>Article 95(1) PSD2 requires payment service providers to adopt appropriate mitigation measures and controls mechanisms relating to the payment services they provide. It also requires the establishment and maintenance of effective incident management procedures including for the detection and classification of major operational and security incidents.</i></p> <p><i>Article 96 PSD2 establishes an incident notification scheme, which foresees that payment service providers 'shall report without undue delay any major operational or security incident to their competent authority in the Member State'.</i></p> <p><i>Article 96 PSD2 also requires payment services providers to inform its payment service users where the incident has or may have an impact on the financial interests of the user.</i></p>	<p><i>Payment service providers are encompassed within <b>Annex II of the NIS Directive as part of the financial services sector.</b> However, as Article 1(7) NIS Directive foresees that where a sector-specific Union legal act requires an OES either to ensure the security of his network and information systems or to notify incidents, that act shall apply provided that the requirements are at least equivalent. Considering that the security and notification requirements prescribed in <b>Articles 95 and 96 PSD2 are equivalent,</b> these provisions are <i>lex specialis</i> to the NIS Directive. Hence, there is <b>no coherence issue.</b></i></p>

In 2018, the Commission put forward a proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research **Competence Centre** and the Network of National

Coordination Centres<sup>17</sup>. The initiative aims to better target and coordinate available funding from the EU budget and Member State contributions for cybersecurity cooperation, capacity and infrastructure building as well as research and innovation. The competence centre should become the main body that would manage EU financial resources dedicated to cybersecurity research under two proposed programmes – **Digital Europe and Horizon Europe** – within the next multiannual financial framework, for 2021-2027. These programmes are pooling more EU and national funding for cybersecurity research, innovation and infrastructure, cyber defence, and the EU’s cybersecurity industry. The Commission proposed to invest €2 billion specifically on cybersecurity. Trialogue negotiations are currently ongoing as part of the adoption procedure of the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

In 2017, the Commission adopted a Joint Communication to the European Parliament and the Council on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, setting a **common approach to cybersecurity with resilience-building**, rapid response and effective deterrence.<sup>18</sup> Proposals to support this through building essential capacities are pending adoption.<sup>19</sup>

Given the ongoing roll-out of the 5G infrastructure across the EU and the potential dependence of many critical services on 5G networks, the consequences of systemic and widespread disruption would be particularly serious. The process put in place by the Commission’s 2019 Recommendation on the **Cybersecurity of 5G networks**<sup>20</sup> has led to Member State action on the measures set out in a 5G toolbox, as reflected in the report on the implementation of the Toolbox adopted in July 2020<sup>21</sup>. The Recommendation foresees its review in the last quarter of 2020.<sup>22</sup>

EU institutions, bodies and agencies (EU-I), with CERT-EU and ENISA’s help, are considering how to prepare better for future incidents and crises, including through the implementation of the Blueprint Recommendation, the development of the Member State **Cyber Crises Liaison Organisation Network (“CyCLONE”) and Cyber Europe incident and crisis management exercises** for the public and private sectors. CyCLONE is notably intended to: (i) facilitate trust building, preparedness, situational awareness and crisis management between national relevant competent authorities; (ii) interact with both the technical (i.e., CSIRT Network) and the EU political level on how to manage large-scale cybersecurity incidents and crises; (iii) support national and EU political level to make an informed decision in large-scale cybersecurity incidents and crises, while avoiding unnecessary escalations to EU level political crisis mechanisms when the

---

<sup>17</sup> COM (2018) 630 final, of 12.9.2018: <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research>

<sup>18</sup> JOIN (2017) 450 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2017%3A450%3AFIN>

<sup>19</sup> Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, COM(2018) 630 final, 2018/0328 (COD)

<sup>20</sup> OJ L 88, of 29.3.2019, p 42 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534>

<sup>21</sup> Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity; <https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>

<sup>22</sup> Commission Recommendation on the Cybersecurity of 5G networks C(2019) 2335 final; Commission. Communication on the Secure 5G deployment in the EU: Implementing the EU toolbox COM(2020) 50 final.

impacts can be dealt with by the operational layer. The Commission has also identified the need for a **Joint Cyber Unit** to provide structured and coordinated operational cooperation. Building on the implementation of the Blueprint recommendation<sup>23</sup>, the Joint Cyber Unit could build trust between the different actors in the European cybersecurity ecosystem and offer a key service to Member States from technical, operational and political level and integration of EUI, MS, CyCLONe SOPs, as well as potential synergies with the PESCO projects.

Cybersecurity is also an important component of the *EU framework for countering hybrid threats*<sup>24</sup>, since the adoption of the first Joint Communication on countering hybrid threats a European Union response in 2016, establishing the link with the NIS framework and highlighting the importance of the convergence of risk management approaches and public-private cooperation<sup>25</sup>. Three sectors were prioritised in this context: energy, transport and finance.

In 2013, Europol set up the **European Cybercrime Centre (EC3)**<sup>26</sup> to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. EC3 is involved in high-profile operations and on-the-spot operational-support deployments. EC3 publishes the annual Internet Organised Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime.

By the end of 2020, the Commission will also adopt a **new cybersecurity strategy – a cybersecurity charter for the EU**, setting out a comprehensive vision, including the role that the NIS legal framework should play.

---

<sup>23</sup> Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239, 19.9.2017.

<sup>24</sup> Defined as a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.

<sup>25</sup> JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response JOIN/2016/018 final.

<sup>26</sup> <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>

**ANNEX 8: OVERVIEW OF POLICY OPTIONS**

Specific policy objectives (SPO)	Policy options				
<p><b>SPO1:</b> Ensure that entities in all sectors that are dependent on network and information systems and that provide key services to the economy and society as a whole are required to take cybersecurity measures and report incidents with a view to increasing the overall level of cyber resilience throughout the internal market</p> <p><b>SPO2:</b> Ensure that all</p>	<p><b>Policy option 0 – maintaining status quo</b></p>	<p><b>Policy option 1 – non-legislative measures to align the transposition of the NIS Directive</b></p>	<p><b>Policy option 2 – Limited changes to the current NIS Directive for further harmonization</b></p>	<p><b>Policy option 3 – Systemic and structural changes to the NIS Directive (new directive)</b></p>	
		<p>Maintaining the scope, requirements and obligations. Continue existing work of the Cooperation Group and the CSIRTs network.</p>	<p>Maintaining the scope, requirements and obligation, while providing sector-specific guidance via the Cooperation Group or by the Commission directly</p>	<p>Bring additional sectors, subsectors and services under the scope within the existing two categories covered by the NIS Directive (OES and DSP)</p>	<p>Bring additional sectors, subsectors and services under the scope, while further refining and simplifying the categories of entities covered by the NIS framework depending on their importance and criticality (i.e. essential and important), and consequently differentiating the particular requirements and supervisory regime imposed on those.</p>
			<p>Guidelines on OES</p>	<p>Harmonize</p>	<p>Abandon identification and</p>
				<p>essential</p>	

Specific policy objectives (SPO)	Policy options			
<p>entities that are active in sectors covered by the NIS legal framework and that are similar in size and have a comparable role are subject to the same regulatory regime (are either inside or outside the scope) no matter which jurisdiction they fall within the EU</p>	<p><b>Policy option 0 – the maintaining status quo</b></p>			
	<p><b>Policy option 1 – non-legislative measures to align the transposition of the NIS Directive</b></p>	<p>identification and coverage of DSPs</p>		
	<p><b>Policy option 2 – Limited changes to the current NIS Directive for further harmonization</b></p>	<p>services and identification thresholds.</p>		
	<p><b>Policy option 3 – Systemic and structural changes to the NIS Directive (new directive)</b></p>	<p>introduce uniform criteria for all entities operating in the sectors and subsectors or providing services covered under the NIS scope, excluding micro or small size enterprises.</p> <p>Entities which are micro or small, but provide services as a sole provider in a Member State or a potential disruption of which could have an impact on the public safety or health would also fall within the NIS scope. Member States would also be able to include in the NIS scope micro and small-size entities in the sectors and services covered by the NIS framework justified on the basis of their importance at</p>		



Specific policy objectives (SPO)	Policy options			
	<p><b>Policy option 0</b> – <i>the maintaining status quo</i></p>			<p><b>Policy option 3</b> – <i>Systemic and structural changes to the NIS Directive (new directive)</i></p> <p>regional or national level for that particular sector or service or for other interdependent sectors.</p>
	<p><b>Policy option 1</b> – <i>non-legislative measures to align the NIS Directive</i></p>			<p>Establish equal footing for all entities of same criticality/importance, while removing the differences in regulatory regime between the entities which are currently qualified as operators of essential services or digital service providers.</p> <p>Establish a registry of digital service providers operating cross-borders.</p> <p>Further clarify the jurisdiction</p>
	<p><b>Policy option 2</b> – <i>Limited changes to the current NIS Directive for further harmonization</i></p>	<p>Introduce clearer and more explicit definitions for DSPs.</p> <p>Further clarify the jurisdiction rules.</p> <p>Establishing equal footing for OESs and DSPs.</p>		<p>Establish equal footing for all entities of same criticality/importance, while removing the differences in regulatory regime between the entities which are currently qualified as operators of essential services or digital service providers.</p> <p>Establish a registry of digital service providers operating cross-borders.</p> <p>Further clarify the jurisdiction</p>

Policy options	
Specific policy objectives (SPO)	Policy options
	<p><b>Policy option 0 – the maintaining status quo</b></p> <p><b>Policy option 1 – non-legislative measures to align the transition of the NIS Directive</b></p> <p><b>Policy option 2 – Limited changes to the current NIS Directive for further harmonization</b></p> <p><b>Policy option 3 – Systemic and structural changes to the NIS Directive (new directive)</b></p>
<p><b>SPO3:</b> Ensure that all entities that are active in sectors covered by the NIS legal framework must follow aligned obligations based on the concept of risk management when it comes to security measures and must report incidents based on a uniform set of criteria</p> <p><b>SPO4:</b> Ensure that competent authorities enforce the rules laid</p>	<p>rules.</p> <p>Introduce uniform and explicit security and incident reporting requirements, potentially directly applicable to the relevant entities.</p> <p>Introduce more explicit reporting obligations concerning incidents, including towards ENISA.</p>
	<p>Harmonize security and incident reporting requirements</p> <p>Introduce more explicit incident reporting requirements</p> <p>Guidelines on security and incident reporting requirements</p> <p>Guidelines on supervision and</p> <p>Establish principles for application of supervisory measures and penalties,</p> <p>Establish principles, as well as a more granular list of minimum requirements, for</p>

Specific policy objectives (SPO)	Policy options				
<p>down by the legal instrument more effectively through aligned supervisory and enforcement measures</p>	<p><b>Policy option 0 – the maintaining status quo</b></p>	<p><b>Policy option 1 – non-legislative measures to align the transposition of the NIS Directive</b></p>	<p><b>Policy option 2 – Limited changes to the current NIS Directive for further harmonization</b></p>	<p><b>Policy option 3 – Systemic and structural changes to the NIS Directive (new directive)</b></p>	
		<p>enforcement</p>	<p>including general conditions for the application of administrative fines.</p>	<p>supervisory measures and enforcement, tailor-made for each category of entities, depending on the level of importance/criticality of the services provided.</p>	
				<p>Establish general conditions for application of administrative fines and a minimum level thereof.</p>	<p>Establish a peer-review system, including on the implementation of supervisory measures and enforcement.</p>
					<p>Introducing liability rules for natural persons responsible for or acting as a representative of the legal person.</p>

Policy options	
Specific policy objectives (SPO)	Policy option 0 – <i>the maintaining status quo</i>
	Policy option 1 – <i>non-legislative measures to align the transposition of the NIS Directive</i>
	Policy option 2 – <i>Limited changes to the current NIS Directive for further harmonization</i>
	Policy option 3 – <i>Systemic and structural changes to the NIS Directive (new directive)</i>
SPO5: Ensure a comparable level of resources across Member States allocated to competent authorities that would allow	Guidelines on DSPs supervision
	Subject DSPs to the same rules as OES (i.e. remove the light-touch approach and introduce full supervision, including <i>ex-ante</i> , for DSPs).
	Subjecting entities (both operators and digital service providers) qualified under the same category (i.e. essential or important) to the same regulatory regime, including supervision and enforcement.  Important entities would be subject to a light-touch regulatory regime (i.e. only <i>ex-post</i> supervision and lighter requirements on penalties).
	Set up a peer-review mechanism to assess, among others, the capabilities of the Member States.
Incentivise Member States, via the Cooperation Group, and through peer pressure to adequately fund their competent	
Require Member States to take the necessary measures to ensure that the competent authorities have the technical, financial and human resources to fulfil their mandate, and in	

Policy options	
Specific policy objectives (SPO)	Policy options
	<p><b>Policy option 0 – maintaining the status quo</b></p> <p><b>Policy option 1 – non-legislative measures to align the transition of the NIS Directive</b></p> <p><b>Policy option 2 – Limited changes to the current NIS Directive for further harmonization</b></p> <p><b>Policy option 3 – Systemic and structural changes to the NIS Directive (new directive)</b></p>
<p>them to fulfil the core tasks laid out by the NIS framework</p> <p><b>SPO6:</b> Ensure that essential information is exchanged between Member States by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents and by developing a Union joint crisis operational response capacity</p>	<p>authorities and other relevant structures, such as the CSIRTs</p> <p>particular their supervisory and guiding roles</p> <p>Set up specific mandatory mutual assistance and cooperation mechanism when cross-border elements are involved.</p> <p>Incentivise voluntary information sharing through ISACs and PPPs.</p> <p>As part of the national cybersecurity strategy, Member States will be required to develop a policy framework on co-ordinated vulnerability disclosure and designate a national CSIRT as a</p>
	<p>Further develop Standard Operational Procedures (SOPs) by the Cooperation Group and the CSIRTs network.</p> <p>Launching CyCLONe, without a set legal framework.</p>
	<p>Continue existing work of the Cooperation Group and the CSIRTs network</p>

Specific policy objectives (SPO)	Policy options			
	<p><b>Policy option 0</b> – <i>the maintaining status quo</i></p>	<p><b>Policy option 1</b> – <i>non-legislative measures to align the transposition of the NIS Directive</i></p>	<p><b>Policy option 2</b> – <i>Limited changes to the current NIS Directive for further harmonization</i></p>	<p><b>Policy option 3</b> – <i>Systemic and structural changes to the NIS Directive (new directive)</i></p>
	<p>coordinator and facilitator.</p> <p>Adding the role of observatory of the state of cybersecurity in the Union to ENISA.</p> <p>Introducing annual/biennial/regular reports on the state of cybersecurity in the EU.</p> <p>Introducing a crisis management framework, for both national and EU levels, including institutionalising CyCLONe.</p>			

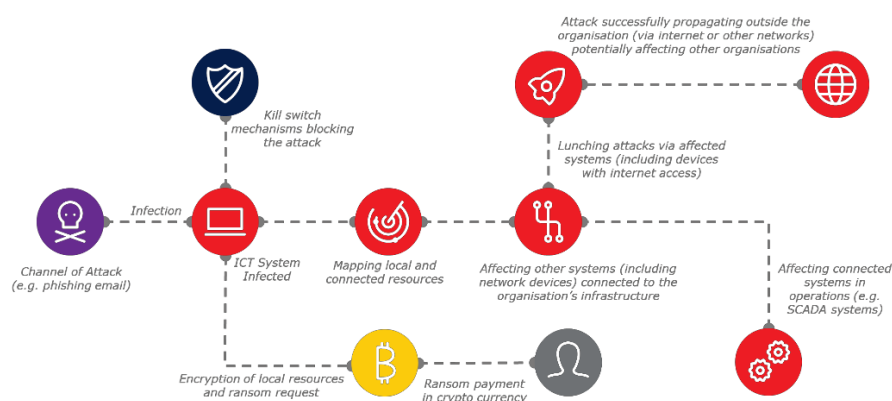
## ANNEX 9: CROSS-SECTOR AND CROSS BORDER PROPAGATION OF INCIDENTS

The 2017 WannaCry ransomware outbreak infected over 230,000 computers in 150 countries on the first day alone<sup>27</sup>. The economic impact of the WannaCry incident is estimated in the order of hundreds of million euros with some cyber risk modelling analysts placing the losses in the order of billions. *For more additional examples and arguments on cross sector and cross border propagation of incidents see annex 10.*

The SamSam ransomware attacks affected different organisations across sectors, the ransomware encrypts data and demand a huge ransom payment in Bitcoin in exchange for the decryption keys. SamSam has attacked different large organisations across sectors, including Transport (e.g. COSCO attack) and Health. As mentioned by the above-referenced ENISA good practices report, SamSam has earned its creator(s) more than 5 million euros since late 2015, a figure that does not take into account revenue losses and system restore costs.

The July 2020 JRC Report<sup>28</sup> also mentions the example of the 2007 coordinated cyber attacks on Estonia, which targeted governmental institutions and bodies, financial entities, telecommunication infrastructure and newspapers: *'a surge of DDoS attacks lasting several weeks caused disruptions at institutional sites and in national online public services and communications, impacting the normal functioning of the national government and society (Schmidt, 2013). These attacks were not highly sophisticated and, due to their nature, did not create any lasting damage to Estonia's digital infrastructure. However, they demonstrated how cyber attacks taking advantage of the digital transformation of governments and society could severely harm an entire country (Joubert, 2012)'*.

The chart below was drafted by ENISA in its good practices on the interdependencies between the OESs and DSPs to illustrate how cross sector and cross border propagation of incidents may occur.<sup>29</sup>



ENISA, in its 2018 good practices, has also pointed to a number of increasing dependencies in certain sectors, such as in the example below concerning the transport sector.<sup>30</sup>

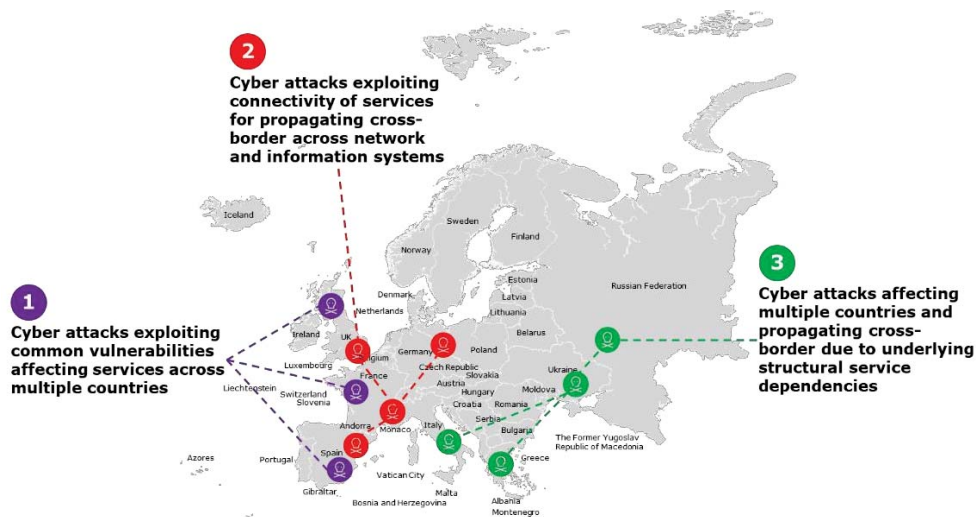
<sup>27</sup> Department of health & Social Care (NHS) UK, 2018.

<sup>28</sup> JRC, July 2020: *Cybersecurity – Our Digital Anchor, a European perspective*

<sup>29</sup> Figure 3, page 12, <https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps>

The JRC Report<sup>31</sup> highlights that ‘From big data to hyperconnectivity, from edge computing to the IoT, to artificial intelligence (AI), quantum computing and blockchain technologies, the ‘nitty-gritty’ details of cybersecurity implementation will always remain field-specific due to specific sectoral constraints. This brings with it inherent risks of a digital society with heterogeneous and inconsistent levels of security. To counteract this, we argue for a coherent, cross-sectoral and cross-societal cybersecurity strategy which can be implemented across all layers of European society.’

Furthermore, ENISA’s 2018 good practices on interdependencies between OES and DSP looked, among others, into cross-border interdependencies, illustrating the types of cyberattacks with cross-border implications in the figure copied below.<sup>32</sup>



Cross-border dependencies therefore pose particular challenges, and would require an effective cross-border cooperation and information sharing.

<sup>30</sup> Figure 6, page 17, idem.

<sup>31</sup> JRC, July 2020: *Cybersecurity – Our Digital Anchor, a European perspective*.

<sup>32</sup> Figure 8, page 21.



## ANNEX 10: EXTRACT FROM THE INTERIM RESULTS OF THE NIS REVIEW STUDY ON A MODELLING FOR COSTS AND BENEFITS

*Note: This is an estimation of costs and benefits which will be incorporated in the final report of the NIS review study<sup>33</sup> due in December 2020/January 2021. The estimation of costs and benefits follows Tool#59 of the EU Better Regulation Tool<sup>34</sup>.*

The main benefit for an intervention aiming to achieve a high level of cyber resilience is **the reduction in cyber incidents** compared to the baseline scenario<sup>35</sup>.

$$\begin{aligned} \text{Economic benefit for option } i &= \text{Reduction in cost of cyber incidents} \\ &= \text{cost of cyber incidents in baseline} \\ &\quad - \text{cost of cyber incident in option } i \end{aligned}$$

The monetary value of cyber incidents relies on different sources based on past incidents. A comprehensive dataset with cyber incident and economic impact is not available. As noted by the Hague report<sup>36</sup>, determining the overall impact of cyber attacks is challenging because there are different reports on cybercrime such as malware, social engineering and fraud to name a few, each source with different methodologies. The lack of a coherent and consistent methodology with standard indicators makes the task challenging. For example, there is abundant anecdotal data of incidents or estimations but varies by scope (sectors, countries, regions), and data by sector can vary remarkably.

However, for the purpose of our estimation at societal level, we need evidence from Europe as a whole. The 2015 Ponemon Institute study on the costs of cybercrime provides the median annualized costs of cybercrime which amounts to USD 5.5 million (EUR 4.63 million).<sup>37</sup> Moreover, there **were almost 450 cybersecurity incidents in 2019 involving** European critical infrastructures like health, finance and energy according to Eurostat<sup>38</sup>.

Based on the median annualized cost of cyber incidents and the number of incidents per year, Figure 1.1 below displays a linear extrapolation of costs of cyber incidents following four assumptions:

Based on the average cost of cyber crime and the number of incidents per year, Figure 1.1 below displays a linear extrapolation of costs of cyber incidents following four assumptions:

1. The annual growth rate of incidents in the baseline scenario follows annual rate of growth in the patterns of digitisation (3%);
2. The annual fall of incidents in option 2 is a conservative 3%;

---

<sup>33</sup> Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665.

<sup>34</sup> [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-59\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-59_en_0.pdf)

<sup>35</sup> Note that as the cost in the baseline is higher than otherwise the difference gives a negative magnitude, but a negative cost is a benefit

<sup>36</sup> [https://www.thehaguesecuritydelta.com/media/com\\_hsd/report/191/document/qe-01-18-515-en-n.pdf](https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf)

<sup>37</sup> [http://www.cnmeonline.com/myresources/hpe/docs/HPE\\_SIEM\\_Analyst\\_Report\\_-\\_2015\\_Cost\\_of\\_Cyber\\_Crime\\_Study\\_-\\_Global.pdf](http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf)

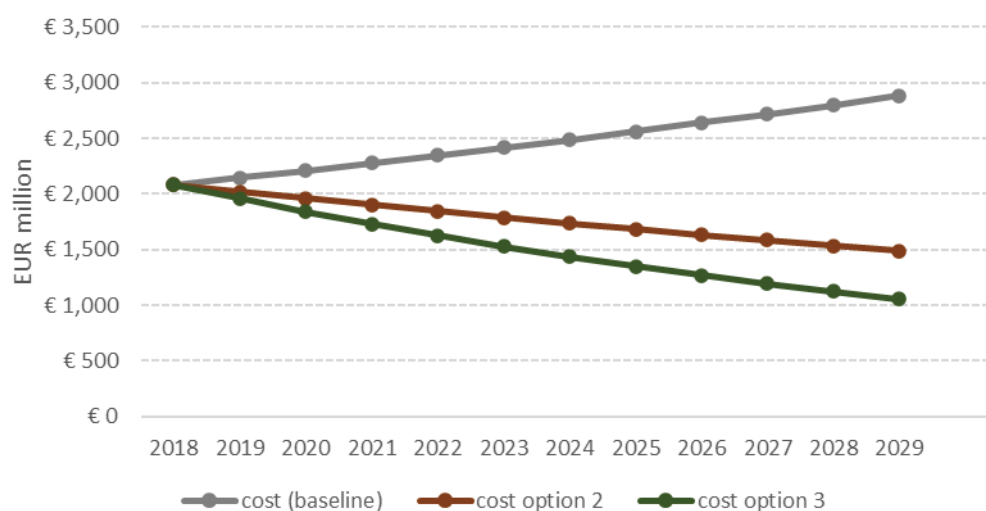
<sup>38</sup> <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>

3. The annual fall of incidents in option 3 is double compared to option 2, namely, 6%
4. The average cost of a cyber incident stays the same in time;
5. We set to 450 the number of incidents in 2018 according to Eurostat figures;

Such assumptions are the most conservative.

[...]

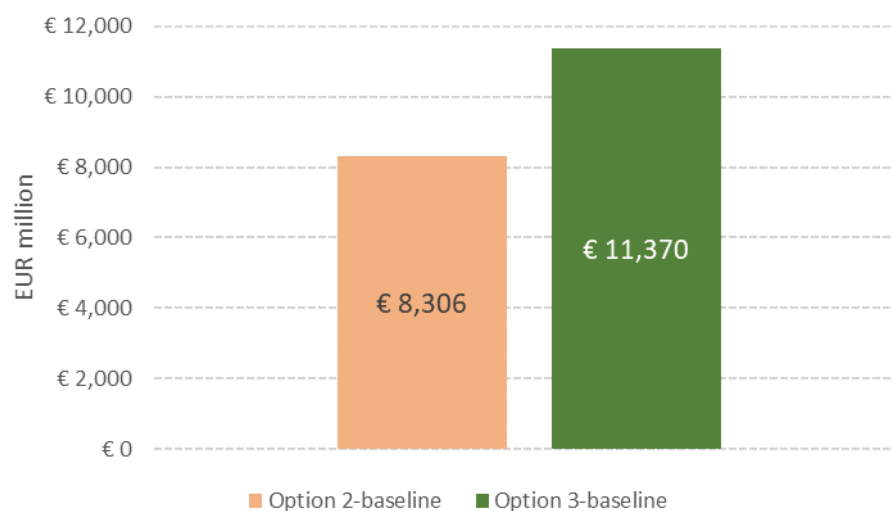
Figure 1.1 The costs of cyber-incidents across scenarios in EUR million (2018-2029)



Source: own elaboration

The expected benefit in option 2 and option 3 are given by the difference of the cost of cyber incidents compared to the baseline over the 10-years period.

Figure 1.2 Saving in cyber incident per option compared to the baseline



Source: own elaboration

**In sum, option 3 is the most impactful with a reduction in cost of cyber incidents by EUR 11.3 billion while option 2 by EUR 8.3 billion.**

**ANNEX 11: LIST OF INDICATORS TO MONITOR HIGH-LEVEL PROGRESS TOWARDS GENERAL OBJECTIVES**

<b>General objectives</b>	<b>Monitoring indicators</b>	<b>Expected targets</b>	<b>Source of data</b>	<b>Frequency of data gathering</b>
<p><b><i>Increase the level of cyber resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors</i></b></p>	<ol style="list-style-type: none"> <li>1. Comparable ICT security spending across sectors and Member States</li> <li>2. Results of random assessments at EU level of cybersecurity capabilities and implementation of cybersecurity policies of 2 key entities per Member State per NIS sector and types of service in at least five Member States (<i>part of the State of Cybersecurity in the Union Report</i>)</li> <li>3. Findings of peer-review mechanism visits as regards the level of NIS compliance and cybersecurity capabilities across the EU</li> <li>4. Overall set of indicators across the EU of the regular business resilience survey</li> </ol>	<ol style="list-style-type: none"> <li>1. Sector-specific ICT security spending as a percentage of ICT spending across Member States deviating with less than 1% from the average sectorial security spendings</li> <li>2. Positive findings on compliance with NIS requirements and level of capabilities (<i>i.e. technical, financial and human</i>) random sector or service-specific assessments of cybersecurity policies of key entities in at least five Member States</li> <li>3. Regular progress found by peer-</li> </ol>	<ol style="list-style-type: none"> <li>1. ENISA data set based on outcomes of framework contract on investment on cybersecurity</li> <li>2. Data gathered for the report on the State of Cybersecurity in the Union (ENISA)</li> <li>3. Peer-review reports</li> <li>4. Annual cyber resilience business survey</li> </ol>	<ol style="list-style-type: none"> <li>1. Annual</li> <li>2. Every two years</li> <li>3. Annual (different sets of Member States per year)</li> <li>4. Annual</li> </ol>

<i>General objectives</i>	<i>Monitoring indicators</i>	<i>Expected targets</i>	<i>Source of data</i>	<i>Frequency of data gathering</i>
<b><i>Reduce inconsistencies in the resilience across the internal market in the sectors already covered by the Directive</i></b>	<p>1. ICT security spending per sector and type of service per Member State as a percentage of IT spending and revenues</p> <p>2. Results of comparative assessments per sectors and types of services per Member State of cybersecurity capabilities and compliance with the NIS framework (<i>part of the State of Cybersecurity in the Union Report</i>)</p> <p>3. Findings of peer-review mechanism visits as regards the level of NIS compliance and cybersecurity</p>	<p>reviews in the level of cybersecurity capabilities across the EU and rate of follow-up of experts' recommendations</p> <p>4. Cumulative positive trend at EU level on all indicators covered by the regular business resilience survey</p>	<p>1. ENISA data set based on outcomes of framework contract on investment on cybersecurity</p> <p>2. Data gathered for the Report on the State of Cybersecurity in the Union (ENISA)</p>	<p>1. Annual</p> <p>2. Every two years</p> <p>3. Annual (different sets of Member States per year)</p> <p>4. Annual</p>

<i>General objectives</i>	<i>Monitoring indicators</i>	<i>Expected targets</i>	<i>Source of data</i>	<i>Frequency of data gathering</i>
	<p>capabilities across the EU</p> <p>4. Comparative sets of indicators per Member State of the regular business resilience survey</p>	<p>cybersecurity capabilities and NIS compliance in sector or service-specific assessments per Member State</p> <p>3. Regular progress at the level of each Member State found by peer-reviews</p>	<p>3. Peer-review reports</p> <p>4. Annual cyber resilience business survey</p>	
<p><i>Improve the level of joint situational awareness and the collective capability to prepare and respond</i></p>	<p>1. Regularity and comprehensiveness of threat assessments and state of cybersecurity in the union reporting</p> <p>2. Completeness of Member States notifications of relevant NIS data to the Commission and ENISA (e.g. incident notifications, discovered vulnerabilities, exchanges of information, instances when mutual assistance mechanism was applied, etc.)</p> <p>3. Number of time the mutual assistance mechanism was triggered in cross-border cases</p>	<p>1. Accurate threat assessment and comprehensive State of Cybersecurity in the Union Report</p> <p>2. Complete Commission and ENISA databases on NIS relevant data</p> <p>3. Frequent use of mutual assistance mechanism in cross-border cases, including joint supervisory actions.</p>	<p>ENISA and Commission reports</p>	<p>Annual</p>

**ANNEX 12: LIST OF INDICATORS TO MONITOR PROGRESS TOWARDS SPECIFIC OBJECTIVES**

<i>Specific Objectives</i>	<i>Operational objectives</i>	<i>Monitoring indicators</i>	<i>Expected targets</i>	<i>Source of data</i>	<i>Frequency of data gathering</i>
<i>SPO1: Ensure that entities in all sectors that are dependent on network and information systems and that provide key services to the economy and society as a whole are required to take cybersecurity measures and report incidents with a view to increasing the overall level of cyber resilience throughout the internal market</i>	Ensure awareness of all entities per sector/ service per Member State of inclusion of the NIS scope and corresponding requirements.	Type and number of entities per sector/service per Member State for which supervisory measures were applied by Member States and notification obligations received.	Entities from all sectors and services covered under NIS scope aware of their obligations and subjected to supervisory measures and reporting obligations.	Notifications from Member States to the commission and ENISA	Every two years
<i>SPO2: Ensure that all entities that are active in sectors covered by the NIS legal framework and that are similar in size/play comparable role in the market are subject to the same regulatory regime (are either</i>	1. Ensure that all similar entities from sectors and services under NIS scope and of medium and large size are subject to the same NIS requirements, tested by random checks/surveys 2. Exceptions on the basis of scarce provision of	1. Random surveys/checks on a representative sample of entities per Member State and per sector/type of service confirming that similar entities (type and size)	1. Confirmed awareness and compliance check for a representative sample per Member State of entities falling under the NIS scope. 2. Minimum 4 cases per year where an entity operating in more	1. ENISA and Commission research and data based on Member States' notifications and targeted surveys 2. Cyber	Annual

<i>Specific Objectives</i>	<i>Operational objectives</i>	<i>Monitoring indicators</i>	<i>Expected targets</i>	<i>Source of data</i>	<i>Frequency of data gathering</i>
<i>inside or outside the scope), no matter under which jurisdiction they fall within the EU</i>	service or potential impact on public health and safety clearly determined and checked randomly	under the NIS scope are aware of the obligations under the NIS framework and/or subjected to supervisory measures by the competent authorities. 2. Number and type of cases where an entity operating in more than one Member State was subject to similar supervisory measures or joint supervisory action	than one Member State was subject to similar supervisory measures on all places of establishment in the EU or to joint supervisory action.	resilience business survey	
<i>SPO3: Ensure that all entities that are active in sectors covered by the NIS legal framework must follow aligned obligations based on the concept of risk management when it comes to security measures and must</i>	1. Ensure compliance with security requirements, including as regards supplier relationship assessment, including via effective supervisory action. 2. Encourage/support stable investment in	1. Number and quality/weight of elements provided by the NIS framework and included in the security measures at the level of entities operating in the sectors or providing	1. Over 50% of businesses per sector/service under NIS scope respondent to the cyber resilience survey confirm an implementation of all elements provided by NIS for security measures, including	1. Cyber resilience business survey 2. Idem 3. Member States notifications to the Commission.	1-4 Annual 5 – one-off, two years since the entry into force of the new NIS legal act

<i>Specific Objectives</i>	<i>Operational objectives</i>	<i>Monitoring indicators</i>	<i>Expected targets</i>	<i>Source of data</i>	<i>Frequency of data gathering</i>
<p><i>report incidents based on a uniform set of criteria</i></p>	<p>cybersecurity resources, including automated security tools at the level of organisations.</p> <p>3. Establish/reinforce the setting at the level of competent authorities to ensure incident notification following the NIS requirements on content, format and frequency, as well as voluntary reporting of near misses and vulnerabilities.</p> <p>4. Establish the notification channels and platforms for the submission of aggregated data on incidents and other notified events by the single points of contact (SPOCs) to ENISA</p> <p>5. Establish and implement policies at Member States level for supply</p>	<p>the services under the NIS scope.</p> <p>2. ICT security per investment of sector/type of service across Member States, including investment in automated security tools.</p> <p>3. Number and type of incidents and other events per sector or type of service under NIS scope notified to the competent authorities and by the latter to the Commission.</p> <p>4. Completeness and quality of aggregated incident-related submitted by the SPOCs to ENISA</p> <p>5. Adopted policies on</p>	<p>supplier relationship assessment.</p> <p>2. Over 60% of businesses per sector/service under NIS scope respondent to the cyber resilience survey confirm investments in automated security tools.</p> <p>3. All competent authorities report significant incidents to the Commission for over half of the essential sectors and services under NIS scope.</p> <p>4. Quality real-time aggregated data submitted by SPOCs of all Member States to ENISA.</p> <p>5. Supply chain policies implemented in each Member State</p>	<p>4. SPOCs submissions to ENISA</p> <p>5. Member States' notifications in the Cooperation Group and peer reviews</p>	



Specific Objectives	Operational objectives	Monitoring indicators	Expected targets	Source of data	Frequency of data gathering
<p><i>SPO4: Ensure that competent authorities enforce the rules laid down by the legal instrument more effectively through supervisory aligned enforcement and measures</i></p>	<p>chain security</p> <ol style="list-style-type: none"> <li>1. Ensure alignment of minimum requirements for supervisory action by the competent authorities for essential entities and effective application thereof.</li> <li>2. Provide for a minimum list of sanctions for non-compliance of essential entities with the NIS requirements and ensure effective application thereof.</li> <li>3. Provide for and apply administrative fines for non-compliance with NIS requirements of essential entities with a maximum as provided by the NIS legal act.</li> </ol>	<p>supply chain security developed at Member States and modalities of implementation</p> <ol style="list-style-type: none"> <li>1. Average number, average frequency, type and prioritisation criteria for supervisory actions conducted by competent authorities per Member State per sector/service under the NIS scope.</li> <li>2. Average number and type of sanctions, other than administrative fines, applied across sectors by competent authorities in each Member State.</li> <li>3. Number and level of administrative</li> </ol>	<ol style="list-style-type: none"> <li>1. Consistent application at Member State level of supervisory action covering all sectors/services under NIS scope based on established prioritisation and randomisation criteria.</li> <li>2. Consistent application across Member States of sanctions other than administrative fines for non-compliance with NIS requirements.</li> <li>3. Enforcement of significant administrative fines for the most serious</li> </ol>	<p>Member States notifications to the Commission or ENISA + cyber resilience business survey + results of peer-reviews.</p>	<p>Every two years</p>

Specific Objectives	Operational objectives	Monitoring indicators	Expected targets	Source of data	Frequency of data gathering
	4. Ensure effective <i>ex post</i> supervision for important entities.	fines applied in the Member States for non-compliance and type of violation for which they were enforced. 4. Number and type of supervisory action applied to important entities from a representative sample of sectors/services under the NIS scope and their follow-up.	breaches of the NIS requirements. 4. Supervisory action applied <i>ex post</i> to a representative sample of important entities across Member States.		
<b>SPO5:</b> <i>Ensure a comparable level of resources across Member States allocated to competent authorities that would allow them to fulfil the core tasks laid out by the NIS framework</i>	Ensure that cybersecurity policies are prioritised at political level in each Member State and that the competent authorities, CSIRTs, SPOCs and the crisis management designated authorities have adequate technical, human and financial resources to effectively fulfil the tasks	Level of cybersecurity capabilities in each Member State reflected through: <ul style="list-style-type: none"> <li>• capacity to conduct supervisory action covering all sectors/services under the NIS scope;</li> <li>• provide support to</li> </ul>	High level of capabilities in at least the points enumerated under the ‘monitoring indicators’	peer-review and ENISA and Commission assessments	continuous

<i>Specific Objectives</i>	<i>Operational objectives</i>	<i>Monitoring indicators</i>	<i>Expected targets</i>	<i>Source of data</i>	<i>Frequency of data gathering</i>
	<p>provided by the NIS framework</p>	<p>businesses on cybersecurity measures and policies;</p> <ul style="list-style-type: none"> <li>• enforce sanctions in case of non-compliance;</li> <li>• develop effective and innovative policies in areas like supply chain security and coordinated vulnerability disclosure;</li> <li>• investment in R&amp;D;</li> <li>• proactive participation in operational cooperation with other Member States, such as mutual assistance mechanisms, public private partnerships, participation in the</li> </ul>			

Specific Objectives	Operational objectives	Monitoring indicators	Expected targets	Source of data	Frequency of data gathering
<p><b>SPO6:</b> <i>Ensure that essential information is exchanged between Member States by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents and by developing a Union joint operational crisis response capacity</i></p>	<ol style="list-style-type: none"> <li>1. Ensure effective operational exchanges among Member States' authorities.</li> <li>2. Ensure the setting up of coordinated vulnerability disclosure policies across Member States</li> <li>3. Incentivise the setting up of sector-specific and cross-sector ISACs with public authorities participation and other public private partnerships</li> <li>4. Set up a crisis management framework at national and EU levels and institutionalising of EU-CyCLONe</li> </ol>	<p>CSIRTs network, etc.</p> <ol style="list-style-type: none"> <li>1. Number of instances when the mutual assistance mechanism was triggered in cross-border cases and number of joint supervision actions.</li> <li>2. Number of coordinated vulnerability disclosure policies set up at the level of Member States, number of national CSIRTs designated as coordinators/facilitators + number of discovered vulnerabilities notified to ENISA.</li> <li>3. Number of operational ISACs and their outcomes; number of other</li> </ol>	<ol style="list-style-type: none"> <li>1. Mutual assistance mechanism applied in a relevant number of cases and use of joint supervisory action.</li> <li>2. Coordinated vulnerability disclosure policies set up in all Member States, responsible CSIRTs designated and vulnerabilities discovered notified to ENISA.</li> <li>3. Steady increase across all Member States in number of sector-specific and cross-sector ISACs and other public-private partnerships.</li> <li>4. Crisis management frameworks in place at national level and CyCLONe and</li> </ol>	<p>Submissions of Member States and peer-review ENISA and Commission assessments</p>	<ol style="list-style-type: none"> <li>1. Annual</li> <li>2. One-off: two years after the entry into force of new NIS framework for setting policies and designation of CSIRT and annual monitoring of notifications of vulnerabilities discovered.</li> <li>3. Every two years</li> <li>4. One-off for the setting up of the frameworks: two years after the entry into force of the new NIS legal act and</li> </ol>

<i>Specific Objectives</i>	<i>Operational objectives</i>	<i>Monitoring indicators</i>	<i>Expected targets</i>	<i>Source of data</i>	<i>Frequency of data gathering</i>
		<p>public private partnerships.</p> <p>4. Number of national authorities designated and procedures in place for crisis management national framework + extent of participation in CyCLONE</p>	<p>dedicated Cooperation Group fully functional.</p>		<p>continuous monitoring of operationally.</p>