EUROPEAN
COMMISSION

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

Glossary: acronyms

Term or acronym	*Meaning*
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 *(cloud service model)*
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 *(cloud service model)*
PPP	Private Public Partnership
ROSI	Return of Security Investment
SaaS	Software as a Service *(cloud service model)*
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

Term/concept	***Definition***
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[1] (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.[2] Furthermore, the **EU Security Union Strategy for 2020 to 2025**[3], 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**[4] 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"*.[5]

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"*.[6] 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."*[7]

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.

---

1 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.

2 https://ec.europa.eu/info/publications/2020-commission-work-programme-key-documents_en

3 COM(2020) 605 final, 24 July 2020.

4 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/

5 https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

6 https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html

7 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[8], 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[9], 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.[10] 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.[11] 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.[12] 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.

---

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

9 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

10 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 .

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

12 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.[13]

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.[14] 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.[15]

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[16], 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

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

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

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

[16] 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.[17] 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.[18]

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**[19], 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**[20] (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[21] and the Commission proposal for a Digital Operational Resilience Act for financial services[22] (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.[23] *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')[24] and the GDPR.[25]*

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

---

17 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.

18 COM(2020) 66 final.

19 COM(2020) 605 final, 24 July 2020.

20 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.

21 Commission Implementing Regulation (EU) 2019/1583.

22 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.

23 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)

24 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.

25 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[26] 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.

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.[27] 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

[26] 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.

[27] 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.[28] 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.[29]

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.[30] 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.[31] 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[32] 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

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

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

[30] 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.

[31] These approaches range from very general provisions to very specific measures, such as specifying the minimum length of passwords.

[32] 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?

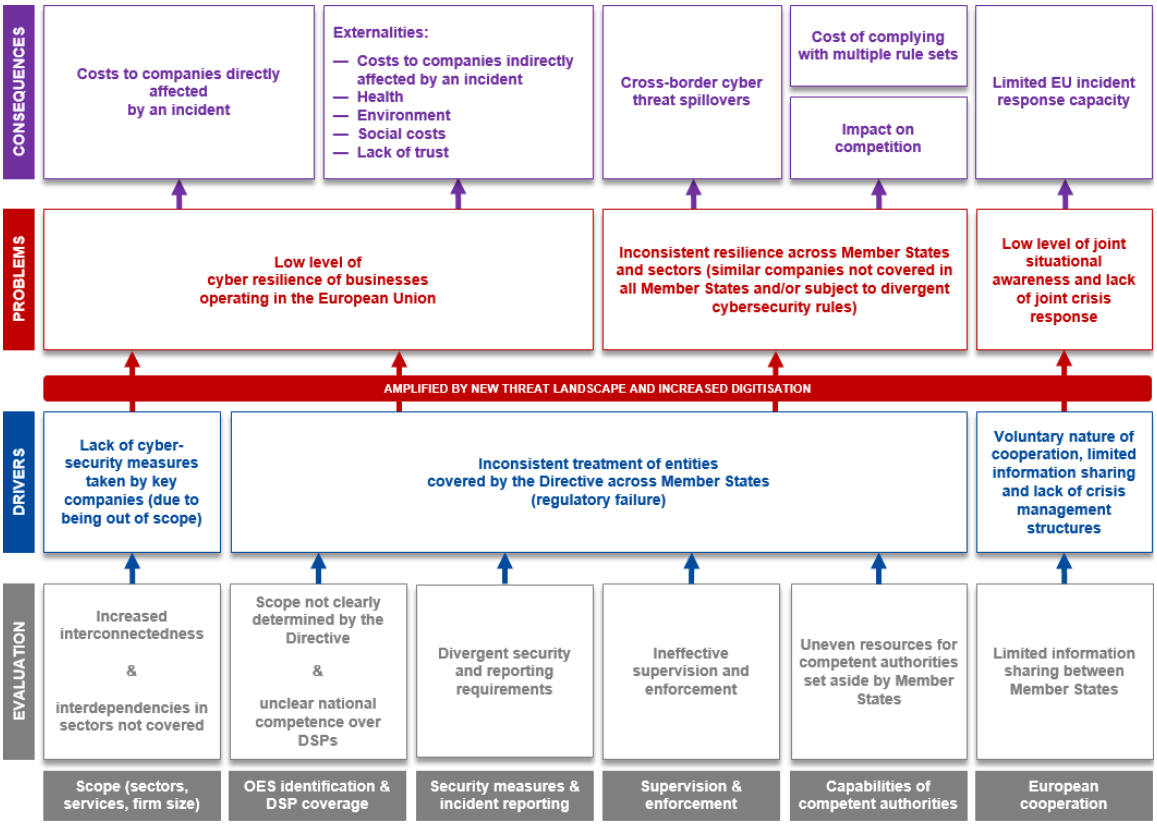


Figure 2: *Outcome of the evaluation, problem drivers, problems and consequences*

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)[33] 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. […]*'[34] The 2020 Digital Economy and Society Index (DESI)[35] 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[36] 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.'[…].*[37] In 2019, one in eight businesses were affected by cyberattacks[38].

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. [39]

---

[33] *Cybersecurity – Our Digital Anchor, a European perspective*, published in July 2020, page 7.

[34] Idem, page 9.

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

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

[37] 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.

[38] 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.

[39] 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[40]. 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[41]). 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.[42] Even for those (sub)sectors already covered by the NIS Directive, the results of the Open Public Consultation (OPC)[43] have shown that on average the level of cybersecurity resilience is assessed by respondents only as medium.[44] 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.[45] Small and medium sized enterprises (SMEs) in particular exhibit a relatively low level of cyber resilience.[46] At the same time, an overwhelming majority of 97 % of the OPC respondents indicated that the cyber threat level has increased since 2016.[47]

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[48].

---

[40] 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.

[41] 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).

[42] Hiscox Cyber Readiness Report 2020: 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.

[43] 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.

[44] 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").

[45] 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.

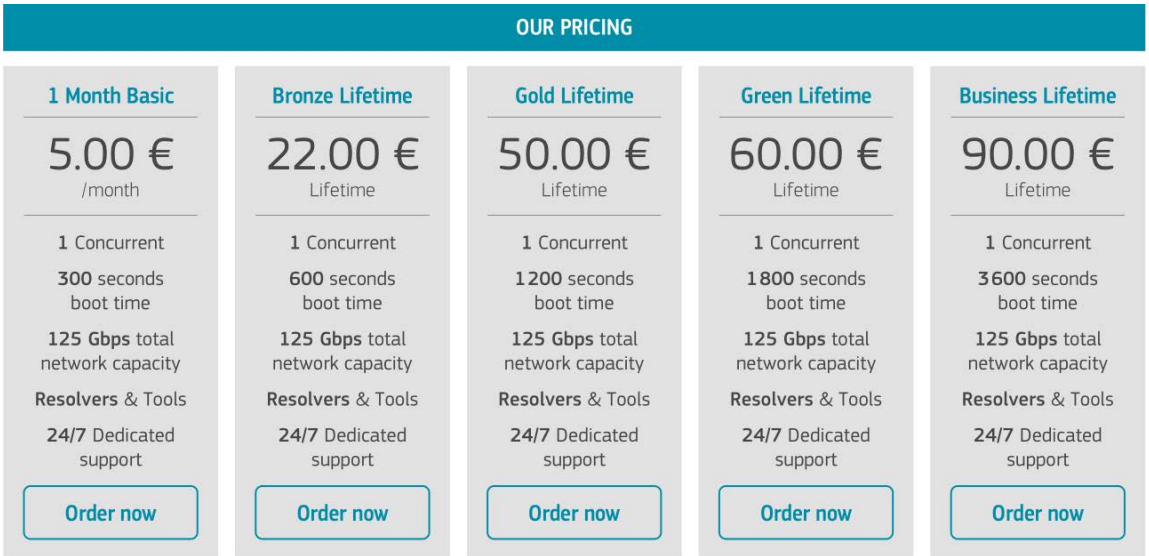
[46] The highest ratings were given by trade associations and DSPs (2.3 each).

[47] 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.

[48] 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.[49] 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.[50] 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.[51] 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.[52] 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.



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

49 PwC (2018): The Global State of Information Security 2018.

50 ESI Thoughtlab (2018): The Cybersecurity Imperative (https://www.protiviti.com/sites/default/files/united_states/insights/cybersecurity_imperative_2018.pdf)

51 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/)

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

Figure 3: *Price list of a service offering DDoS attacks*[53]

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[54] 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).

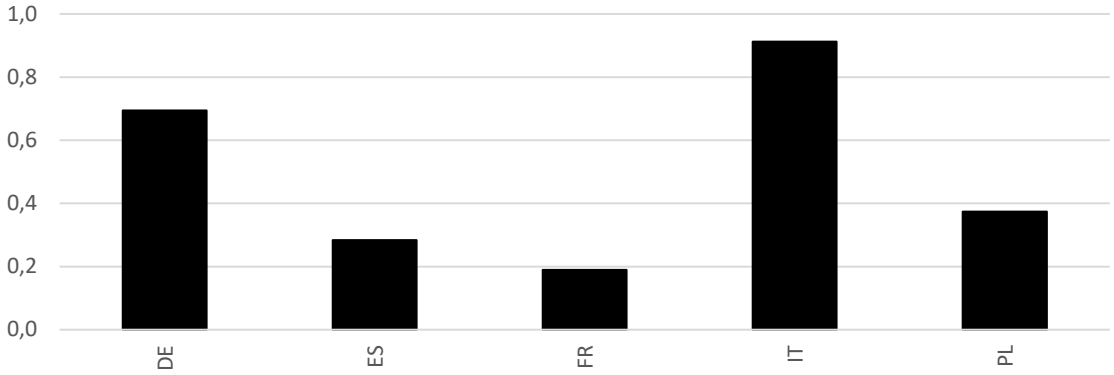


Figure 4: *Number of identified OESs in the five biggest Member States (per 100,000 inhabitants)*

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.[55] 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.[56] It is the very nature of cybersecurity in the value chain that investments undertaken by one company

---

[53] 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

[54] Overall, Member States have reported 15,676 identified OESs to the Commission, 10,897 of which were identified by Finland.

[55] 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.

[56] 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).[57] 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"*.[58] 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"*.[59] 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"*.[60]

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.[61] According to a recent report of the Ponemon Institute on the cost of data breaches[62], 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"*.[63] Respondents to the Commission's inception impact assessment are also very critical of the OES

---

[57] IPACSO: A Coordination Action under the FP7 DG CNECT Trustworthy ICT Program, deliverable D4.1

[58] 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.

[59] 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.

[60] 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.

[61] Conducted by the Commission as part of the NIS review process in 2019-2020.

[62] 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

[63] 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"*.[64] 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"*.[65] Regarding incident reporting requirements, 87 % of respondents feel that the *"different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES"*.[66] 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"*.[67] 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"*.[68]

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[69]. 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[70] only represent a small subset of the incidents taking place within

---

64 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.

65 The statement is supported by stakeholders throughout all categories.

66 However, only 63 % of competent authorities agreed with this statement.

67 Stakeholders throughout all categories disagreed with this statement. Cybersecurity professionals tended to disagree the least, with "only" 64 % disagreeing with the statement.

68 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.

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

70 See Article 10(3) of the NIS Directive.

the EU. Member States have rarely made use of the cross-border notification provisions[71], 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.[72]

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)[73] on European level beyond the sharing of information within the different cooperation fora established by the NIS Directive.[74] 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.[75]

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

[71] Article 14(5) and 16(6) of the NIS Directive.

[72] 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.

[73] 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.

[74] 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.

[75] 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.[76]

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[77] create an incentive for businesses not to limit their exposure to risk (so-called moral hazard).[78] 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.[79] 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.[80]

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.[81] 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[82] but also

[76] 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.

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

[78] Vagle (2020): Cybersecurity and Moral Hazard. Stanford Technology Law Review, Vol. 23:1, p. 71.

[79] 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.

[80] Barbara Filkins (2020) "Spends and Trends: SANS 2020 IT Cybersecurity Spending Survey", SANS Institute: Information Security Reading Room, 450 respondents.

[81] 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.

[82] 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[83]. 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.[84] 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[85], 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.

---

[83] 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.

[84] Article 18 of the NIS Directive.

[85] 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[86], 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.[87] 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[88], 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[89], 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

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

[87] 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.

[88] 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.

[89] 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.[90] 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).[91] 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).[92] 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.[93] To support Member States in carrying out cross-border consultations, the Cooperation Group issued a reference document in July 2018.[94] 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.[95] The main reasons for this lack of engagement are the

[90] 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.

[91] National Cyber Security Index 2018, e-Governance Academy: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

[92] ITU Global Cybersecurity Index 2018: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[93] Article 5(4) of the NIS Directive.

[94] 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.

[95] 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[96], 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*

[96] 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."[97]

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.[98] 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[99] 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.

---

[97] 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/ .

[98] 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.

[99] 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.*

Problem drivers	Specific policy objectives	Policy options			
		PO0 (status quo)	**PO1** (non-legislative)	**PO2** (limited changes)	**PO3** (subst. changes)
DR1: Lack of cybersecurity measures taken by key companies	**SPO1:** 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
DR2.1: Discrepancies in OES identification and DSP coverage	**SPO2:** Similar entities in covered sectors subject to the same regulatory regime		Guidelines on OES identification and coverage of DSPs	Harmonize essential services and identification thresholds.	Replace identification by uniform criteria for all entities, excluding micro or small.
				—Clearer DSP definitions —Clarify jurisdiction rules —Equal footing for OESs and DSPs	—Equal footing for all entities in same category —Registry of cross-border digital service providers —Clear jurisdiction
DR2.2: Inconsistent security measures and reporting requirements	**SPO3:** Entities to follow aligned security and reporting obligations		Guidelines on security and incident reporting requirements	Harmonize security and reporting requirements	—Introduce uniform security and reporting requirements —Explicit incident reporting rules
				Explicit incident reporting requirements	
DR2.3: Ineffective supervision and enforcement	**SPO4:** Competent authorities to enforce more effectively		Guidelines on supervision and enforcement	Principles for supervisory measures and penalties	—Principles + minimum requirements —General conditions + minimum level for fines —Peer-review system —Liability rules for natural persons
			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
DR2.4: Discrepancies in Member State capabilities	**SPO5:** 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
DR3.1: Voluntary nature of cooperation	**SPO6:** 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
DR3.1: Limited information feeding into the existing groups					
DR3.1: 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.[100] 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.[101]

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

[100] 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.

[101] 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.[102]

Currently there is a very low number of reported incidents.[103] 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.[104] 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.[105] 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

[102] 72% considered that the misalignment of the security requirements is a pressing issue.

[103] 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.

[104] 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.

[105] 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.[106] 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[107] 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[108] high-level cross-sectoral crisis coordination process (for the Commission) and the EEAS Crisis Response Mechanism. The EU civil protection mechanism[109], 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**[110], 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')[111].

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

[106] 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.

[107] four of which in the transport sector.

[108] general rapid alert system linking all the European Commission's specialised systems for emergencies.

[109] https://ec.europa.eu/echo/what/civil-protection/mechanism_en .

[110] Article 7(1).

[111] 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** c**ommunication providers** in the European Electronic Communications Code[112] 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).**[113] 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.[114]

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

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

[113] 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.

[114] 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.[115]

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.*

No.	***Sector/type of service***	***Criteria considered in view of inclusion in the NIS scope (in the order of scoring)***	***Qualitative aspects supporting the inclusion in the scope of the NIS framework***
1	Wastewater	• Member States' national policies; • Results of consultations; • COVID-19 crisis.	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. Cyber-attacks on wastewater utilities or process control systems can cause significant

[115] 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	• Digital intensity; • Interdependency with other sectors; • Member States' national policies; • Results of consultations; • COVID-19 crisis.	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	• Digital intensity; • Interdependency with other sectors; • Member States' national policies; • Results of consultations; • COVID-19 crisis.	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	• Digital intensity; • Interdependency with other sectors;	Trust service providers are subject to security and reporting obligations under the eIDAS Regulation, which are

		• Results of consultations.	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. The repeal of these obligations from the eIDAS Regulation and their inclusion under the revised NIS would streamline the legal obligations for those entities.
5	Public electronic communications networks and electronic communications services (insofar as these are publicly available)	• Digital intensity; • Interdependency with other sectors; • Member States' national policies; • Results of consultations; • COVID-19 crisis.	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. 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.
6	Postal and courier services	• COVID-19 crisis • Member States' national	Postal and courier services are key services for businesses,

		policies; • Results of consultations; • Digital intensity; • Interdependency with other sectors	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.
7	Waste management	• Results of consultations; • Member States' national policies; • COVID-19 crisis; • Interdependency with other sectors	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. Damaging or even catastrophic environmental releases may be triggered remotely by cyber attacks.
8	Manufacture, production and distribution of chemicals	• Member States' national policies; • Results of consultations; • Digital intensity	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.[116] 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

[116] 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.[117]
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)	• Member States' national policies; • Results of consultations; • Digital intensity; • Interdependency with other sectors; • COVID-19 crisis	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. Cyber attacks on manufacturing companies can cause considerable disruptions and financial damage along the whole supply chain. As show by a study conducted by Deloitte and MAPI on cyber risks in advanced manufacturing[118], 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. 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

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

[118] https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html .

			national policies of the Member States.
10	Food supply	• Member States' national policies; • Results of consultations; • COVID-19 crisis; • Digital intensity.	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. 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.[119] 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.[120]
11	Social networks	• Results of consultations; • COVID-19 crisis;	Social networks have an increasing importance for societies, ranging from connecting people and

[119] https://www.securityweek.com/cybersecurity-threats-food-supply-chain .
[120] https://www.qad.com/blog/2020/09/why-cybersecurity-matters-in-the-food-and-beverage-supply-chain

		• Digital intensity.	businesses, up to social media and e-commerce, as well as influencing democratic processes and distribution of news and information. In 2020, 3.81 billion people worldwide were using social media. 49% of the total world population are using social networks.[121] Digital consumers spend nearly 2.5 hours on social networks and social messaging every day.[122] According to DESI[123], 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.[124] 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. Social media is primarily used by cybercriminals as an intelligence gathering tool, but it is also a threat vector itself[125], notably when cybercriminals are spreading malware and misinformation.[126] For example, in May 2016, LinkedIn was hacked, and 117 million credentials were exposed. In 2017, Vevo fell

[121] 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

[122] 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/ .

[123] https://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_-_statistics_on_the_use_by_enterprises

[124] https://ec.europa.eu/digital-single-market/en/use-internet .

[125] https://www.bridewellconsulting.com/cyber-trends-for-2020-social-media-attacks .

[126] 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.[127]

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[128], 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.

[127] Idem.

[128] 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).

<table>
<tr><th colspan="2">Sectors and subsectors for the OES currently under the scope of the NIS Directive which will also remain under option 2</th><th colspan="2"><u>New</u> sectors and subsectors for OES considered to be <u>added</u> to the NIS scope</th><th>Types of DSPs currently in the scope of the NIS Directive</th><th><u>New</u> types of DSPs considered to be <u>added</u> to the NIS scope</th></tr>
<tr><td rowspan="5">Energy</td><td>Electricity (supply, distribution, transmission)</td><td rowspan="5">Energy</td><td>Electricity generation</td><td rowspan="5">Online marketplaces</td><td rowspan="5">Social networks</td></tr>
<tr><td>Oil</td><td>(Nominated) electricity market operators</td></tr>
<tr><td rowspan="3">Gas</td><td>Central oil stocking entities[129]</td></tr>
<tr><td>Electricity market participants providing aggregation, demand response or energy storage services[130]</td></tr>
<tr><td>Operators of hydrogen production storage and transmission[131]</td></tr>
<tr><td rowspan="2">Transport</td><td>Air</td><td colspan="2" rowspan="2">Heat production and supply</td><td rowspan="2">Online search engines</td><td rowspan="2">Trust service</td></tr>
<tr><td>Rail</td></tr>
</table>

[129] As defined in point (f) of Article 2 Directive 2009/119/EC.

[130] 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.

[131] Communication "A hydrogen strategy for a climate-neutral Europe".

	Water				providers
	Road				
Banking		Chemicals (manufacture, production and distribution)		Cloud computing services	
Financial market infrastructures		Food supply[132]			
Health (healthcare providers)		Health	EU reference laboratories[133]		
			Entities conducting research and development activities of medicinal products[134]		
		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[135]		Content Delivery Network providers		
	Top Level Domain (TLD) name registers				

[132] 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.

[133] 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.

[134] 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);

[135] 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[136]		
	Postal and courier services		
	Manufacturing (certain subsectors)[137]		
	Public administration[138]		
	Operators of government-owned and privately-owned ground-based infrastructure that support the provision of space-based services[139]		

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

[136] 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.

[137] 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 produces 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.

[138] 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.

[139] 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.[140]

- ✓ The **DSP coverage rules** would remain the same, i.e. there would be no identification process for the DSPs.[141] Further clarifications would be introduced in relation to the **jurisdiction rules**[142].
- ✓ **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[143] 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.[144] 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[145]** 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

[140] See also policy option 3 for an assessment of the alternative measure of harmonisation of identification thresholds.

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

[142] 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.

[143] 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.

[144] Data based on notifications from the Member States pursuant to Article 5(7) of the NIS Directive.

[145] Broadcasting services and emergency communication services are also considered under this sector.

providers operating in 28 of the 31 EU and EEA/EFTA countries.[146]

- ✓ For new sectors considered, the number of entities[147] 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**[148]: 595,233 companies; for **manufacturing, for 8 selected subsectors** (other than chemicals)[149]: 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.[150] In EU households, heating and hot water alone account for 79% of total final energy use.[151] 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%[152]

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

---

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

[147] According to Eurostat data corresponding to 2018, as presented in Annex 3.

[148] 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.

[149] 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.

[150] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_and_heat_statistics&oldid=493775#Derived_heat_production

[151] https://ec.europa.eu/energy/topics/energy-efficiency/heating-and-cooling_en?redir=1

[152] 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.[153] 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[154] 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

[153] taking account of new cyber threats, technological developments or sectorial specificities.
[154] 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[155] 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[156] 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[157] 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.

[155] including secure information sharing tools.
[156] trough guidelines, opinions.
[157] 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.[158] 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

[158] 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.

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

[159] 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)[160]	
Financial market infrastructures		Chemicals (*manufacture, production and distribution)*	
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[161]		
	Entities manufacturing medical devices considered as critical during a public health emergency[162]		

[160] As described under option 2, Table 3, footnote 137.

[161] 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.

[162] 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 produces and medical devices (COM92020)725 final).

Wastewater systems		
Drinking water distribution and supply		
Digital infrastructure	IXP providers	
	DNS service providers[163]	
	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[164]	
Public administration[165]		
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**[166] would be introduced

[163] The definition would be further clarified, as mentioned in option 2.

[164] As in the option 2, the respective provisions of the EECC would be repealed.

[165] As defined in option 2.

[166] 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[167] 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[168], (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

[167] As defined by the Commission Recommendation 2003/361/EC of 6 May 2003.

[168] 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.[169] 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**[170], 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[171]. 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[172] 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.

[169] i.e. the European Electronic Communications Code (Articles 40 and 41) and the eIDAS Regulation (Article 19).

[170] 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.

[171] 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/

[172] 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)[173]; 140 IXPs[174] (with one company usually administering several IXPs); for authoritative DNS resolution: two root name servers[175], 28 major ccTLD entities[176] and a large number of domain name registrars and web hosting companies[177], and for recursive DNS resolution: DNS resolvers provided by most internet service providers[178] 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[179], 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[180], 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.[181]
- According to the 2020 Digital Economy and Society Index (DESI)[182], 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'.[183] Some estimates indicate about 1,700[184] cloud service providers in Europe. Overall, there are only few large companies on the European market: Amazon[185], Microsoft, Google and

[173] one in each Member State plus EURid, which administers .eu
[174] Referenced for 2020. The 140 IXPs are located in the EU, with some being of global importance.
[175] providing authoritative DNS resolution for the root zone, located in the Netherlands and Sweden.
[176] 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.
[177] offering authoritative DNS resolution as part of their domain registration services.
[178] As part of the internet access arrangement. See the data on electronic communication networks and services.
[179] Netmarketshare.com.
[180] Commission estimate of 2019: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168
[181] 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_swd_en.pdf
[182] https://ec.europa.eu/digital-single-market/en/integration-digital-technology
[183] 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.
[184] 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
[185] Biggest player in France, Germany, the UK and the Netherlands.

IBM.[186] 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**[187], 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**[188]: 5,303 medium and large companies; for **manufacturing, for 8 selected subsectors** (other than chemicals)[189]: 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

[186] 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.

[187] Broadcasting services and emergency communication services are also considered under this sector.

[188] 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.

[189] 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[190] 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.[191] In terms of type of applicable **penalties,** the new NIS legal act would set the Member States' obligation to provide for administrative fines[192] 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.[193] 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.

---

[190] 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.

[191] 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.

[192] 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.

[193] 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**.[194] 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:
  - o 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.
  - o 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.

[194] 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.[195] 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**[196] (hereinafter called 'the ECI Directive'), with a view to adopt a proposal by the end of 2020. The aim of the latter is to

[195] *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

[196] 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 then 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.[197] This is acknowledged by further research.[198] The ROSI model finds that the optimal level of security is reached when the cost of security measures equals the costs of security breaches. [199]

---

[197] 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. […]'*

[198] *Security Metrics and Security Investment Models,* Rainer Boehme, International Computer Science Institute, Berkeley, California, USA;

[199] 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.[200] 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.[201]

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[202]. 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.[203]

- ***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

[200] 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).

[201] IPACSO Report, page 12, reference to a study of the Research Triangle Institute in 2006 in the US.

[202] 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.

[203] 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[204], 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[205], 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')[206] 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.**[207] In the banking sector, a survey by Deloitte and FS-ISAC[208] 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 [209] 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

[204] Data still incomplete at the time of the writing of this Impact Assessment report.
[205] i.e. data available in the impact assessment supporting the NIS Directive.
[206] 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/.
[207] 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
[208] 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
[209] 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.[210] 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[211] 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

[210] 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.

[211] 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***.[212] 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

[212] 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[213] 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[214] 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

[213] 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*).

[214] Full Time Equivalent.

concerning the *risk management measures*[215] and the *prevention and mitigation of impact of incidents*.[216] Fewer respondents[217] 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[218] 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.[219] ***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'*[220], 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

[215] 73% for OESs and 56% for DSPs.
[216] 73% for OESs and 56% for DSPs.
[217] 43-49% for OESs and 33-44% for DSPs.
[218] Information security personnel includes in-house and contract full-time equivalents supporting the IT security domains.
[219] https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises#ICT_security_in_EU_enterprises
[220] 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 %).[221] 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.[222]

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

[222] 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[223] 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[224] **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.[225] 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***[226] to be ***EUR 3.5 million in 2018***, an increase of 6.4 % over the previous year[227], 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%**[228] **to 22%**[229]) would lead to a **proportionate benefit of such investments** and even considerably exceed the costs for some sectors.

---

[223] http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

[224] 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].

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

[226] 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.

[227] 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

[228] sectors already covered by the NIS framework.

[229] 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[230], 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[231] 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.[232]

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.

---

[230] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises

[231] 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

[232] *Cyber incidents, security measures and _financial returns: Empirical evidence from Dutch firms*, Milena Dinkovay_, Ramy El-Dardiryy 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.[233] Financial entities would be required to put in place basic security measures.[234] 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[235] 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 Centre 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.

[233] such as identification, protection and prevention, detection, response and recovery, learning and evolving and communication.

[234] e.g. set-up and maintain resilient ICT systems and tools that minimise ICT risk, business continuity policies and disaster and recovery, etc.

[235] 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.[236] 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.

[236] ***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

- ✓ 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.[237]

- **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[238], 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).[239] 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.[240] According to Eurostat[241], 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

[237] The respondents to the OPC rate the level of preparedness of European SMEs with an average of 2.17 out of 5.
[238] COM(2020) 605 final, 24 July 2020.
[239] https://ec.europa.eu/eurostat/web/regions/background
[240] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Total_general_government_expenditure
[241] 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.[242] 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

[242] 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[243].

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.

[243] 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[244] 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.[245] These costs could however be partially supported through the Digital Europe Programme – Multiannual Financial Framework.[246]

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

[244] Via SPOCs.

[245] e.g. travel and accommodation costs, daily allowances, expert days spent in one week country visits, preparation work, drafting work, etc.

[246] 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[247] 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.[248] 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.[249] 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.

---

[247] Cybersecurity – Our Digital Anchor, a European perspective, published in July 2020.

[248] '*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 […].*'

[249] 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 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.[250]

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.

[250] 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**	✗	✓✓
Total	**0**	✓✓✓✓✓✓✓✓ ✗	✓✓✓✓✓✓✓✓✓ ✓✓✓

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[251] and trust service providers[252] 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.

[251] 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.

[252] 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.

REFIT Cost Savings – Preferred Option		
Description	***Amount***	***Comments***
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[253] and implementation of cybersecurity policies within the organisation, measured through indicators concerning the strength and sophistication of security measures, control and

[253] 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[254], resources available and fluctuations thereof, interaction with public authorities, occurrence, handling and impact of incidents.

[254] 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.