



Brussels, 16.12.2020  
SWD(2020) 345 final

PART 2/3

**COMMISSION STAFF WORKING DOCUMENT**

**IMPACT ASSESSMENT REPORT**

*Accompanying the document*

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

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

## Table of Contents

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

## Glossary

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

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

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

## ANNEXES

### ANNEX 1: PROCEDURAL INFORMATION

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

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

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

#### 2. **Organisation and timing**

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

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

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

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

#### 3. **Consultation of the RSB**

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

#### 4. **Evidence, sources and quality**

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

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

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

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

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

---

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

## ANNEX 2: STAKEHOLDER CONSULTATION

### 1. Introduction

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

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

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

### 2. Consultation scope and objectives

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

The stakeholder consultation has two objectives:

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

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

### 3. Consultation activities

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

The following consultation activities were organised:

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



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

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

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

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

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

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

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

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

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

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

##### ✓ **Profile of respondents**

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

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

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

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

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

#### ✓ **Cyber threat landscape**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#### ✓ SMEs

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

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

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

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

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

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

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

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

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

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

#### ✓ **Security requirements**

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

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

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



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

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

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

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

#### ✓ **Incident notification**

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

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

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

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

As the OPC respondents were asked to think about ways of improving the information available to cybersecurity authorities on national level, they were then asked to describe which information gathered by national authorities should be made available at EU to improve common situational awareness. The most frequent information types given, in order of importance, were as follows:

- Aggregated statistical data describing the current cyber threat landscape.
- Top threats and top incidents in terms of occurrence.
- Emerging cyber threats.
- Incidents with cross-border relevance.
- Indicator of Compromise (IOC) notifications based on level of seriousness.
- Attacks on sectors, attack vectors, critical vulnerabilities.
- Best practices on risk identification, remediation and/or mitigation.

#### ✓ **Information sharing**

The respondents were asked to evaluate the level of incident-related information sharing between Member States. Setting aside those not in the position to reply, it appears that the level of information-sharing between MS requires substantial improvement as below chart presents. A larger proportion OPC respondents were critical than those assessing this aspect positively.

OPC respondents were also asked about ways in which organisations could be incentivised to share more information with cybersecurity authorities on a voluntary basis. The most frequent suggestions made by the respondents revolved around the **simplification of reporting processes** guaranteeing anonymity, as well as **free and transparent access to anonymised reporting information**.

The respondents were also asked to rate the level of information exchange on cybersecurity between organisations in their respective sectors. Around three-quarters of the respondents were unable to provide a rating. The level of information exchange was ranked the highest among organisations in the financial and banking sectors and the lowest among organisations in the health sector. A third of the respondents indicated a low level of information exchange across sectors, while a further 8.7% indicating a very low level. Just over a quarter of the respondents (26.7%) indicated a medium level of information exchange across sectors. Very few respondents thought the level of information exchange across sectors was high (3.4% or 7 out of 206 respondents).

The OPC respondents were then asked how the level of information exchange between companies could be improved within Member States but also across the European Union. The most frequent suggestions were made, in order of importance:

- Centralising the information sharing duties either at EU or national level.
- Greater role for CSIRTs: establishing trusted CSIRTs and encourage sectoral-level CSIRTs to foster national and international information-exchange.
- National boards of experts meeting regularly to exchange information and best practices on mitigation and remediation.
- Through structured and trust-based mechanisms ensuring anonymous information

sharing by competent authorities.

- Developing European-level ISACs at sectoral level.
- Industry-led initiatives for intra-sector information sharing between OES.
- Making it a legal obligation through an EU-level regulatory activity.
- Promote the use of robust, automated information sharing architectures, capable of turning threat indicators into security protections in near-real time.

#### ✓ **Enforcement**

Most respondents did not know or were unable to answer whether: Member States are effectively enforcing the compliance of OES (45.1%); Member States are effectively enforcing the compliance of DSPs (62.1%); the types and levels of penalties set by Member States are effective, proportionate and dissuasive (50.5%); and whether there is a sufficient degree of alignment of penalty levels between the different Member States (63.6%).

#### ✓ **Efficiency**

Most stakeholders agreed to some extent that **the effects of the NIS Directive have been achieved at a reasonable cost**. In particular, trade associations (42.6%, plus 7.4% to a large extent), OESs & DSPs (40.4%, plus 17.5% to a large extent), NCAs & CSIRTs (35.7%, plus 14.3% to a large extent), cybersecurity professionals (38.1%, plus 9.5% to a large extent), and citizens (50%). The majority of stakeholders thought that the **NIS Directive had medium to high impact on the overall level of resilience against cyber-threats across the EU**. This opinion was shared especially among the OES & DSPs (33.3% high impact and 38.6% medium impact), Trade associations (27.9% high impact and 27.9% medium impact), cybersecurity professionals (14.3% high impact and 38.1% medium impact) and citizens (20% high impact and (70% medium impact).

#### ✓ **Coherence with other legal instruments**

The majority of trade associations, OESs & DSPs, and citizens rated the **coherence of the NIS Directive** as being medium and high. On the other hand, most of cybersecurity professionals and NCAs & CSIRTs thought the coherence was low and very low.

#### ✓ **Vulnerability discovery and coordinated vulnerability disclosure**

The respondents were asked to evaluate the level of effectiveness of national policies that are making vulnerability information available in a timelier manner. Just under a quarter of the OPC respondents (24.8%) thought their level of effectiveness were medium, while 15.5% of the respondents rated the national disclosure policies as low or very low.

The OPC respondents were asked if their organisation have implemented a coordinated vulnerability disclosure policy. A significant proportion of the respondents did not respond or indicated this did not apply to them or their organisation (48%, 99 out of 206 respondents). 57 respondents went on to argue that national authorities such as CSIRTs could take proactive measures to discover vulnerabilities in ICT products and services provided by private companies.

### ANNEX 3: WHO IS AFFECTED AND HOW?

#### 1. **Practical implications of the initiative**

The initiative would affect the following stakeholders:

- Private sector/industry
- Public administration (from the perspective of being included under the NIS scope)
- Competent authorities (including CSIRTs and SPOCs)

ENISA would also be affected in particular in policy option 3, which considers a number of additional measures within the limits of ENISA's mandate.

The assessment of impacts, including costs and benefits, for all the above-mentioned categories of stakeholders is covered by the main text of the Impact Assessment. This annex provides more detailed background information on the way the economic impact was analysed as regards the private sector/industry, for all the sectors, subsectors and services considered in the policy options, as well as public administration.

##### ➤ *Private sector/industry*

The NIS Directive is covering under its scope 7 sectors (each including subsectors and/or services) and types of digital services, as listed in Annexes II and III. In order to determine the potential impact of the policy options on businesses, the impact assessment considered the following steps:

- i. Determining the breadth of the (sub)sectors and services that would fall within the NIS scope, starting with the existing (sub)sectors and services, followed by the ones considered to be added in policy options 2 and 3.
- ii. Within these sectors, determining the extent of medium and large companies that would be covered under the NIS scope in policy option 3.
- iii. Estimating the average percentage of ICT security spending out of ICT spending and total revenue per sector and the likely evolution thereof.

Further, the impact assessment estimated the costs and benefits at the level of organisations, including the particular economic impact on SMEs, as also reflected in section 2 of this annex and then respective costs and benefits tables.

The data on the entities active in the (sub)sectors and services covered by or considered for the NIS scope are presented below in tables summarising the cross-sector estimates, as well as further below in a more detailed format, explaining the results presented in the summary tables. The analysis relied mainly on Eurostat and DESI data. Similar data was not available across the EU for all (sub)sectors or services analysed. Furthermore, the data was often available in aggregate forms which do not always entirely match the types of entities defined under the NIS scope, therefore in most cases the overall figures represent an overestimate. Whenever systematic data on number of companies and turnover was not available, proxies were used to the extent possible, including data or information on market structure or market shares. The data and estimates below provide therefore a meaningful, yet not comprehensive overview of the above-mentioned metrics. To the extent available, sector-specific data is provided on medium and large entities that would be covered as a rule by the NIS scope in policy option 3. Furthermore, for the sectors currently covered by the NIS scope, a comparison is being made with the number of OES notified by the Member States.

Mention should be made that in policy option 2, the identification process for OESs would be maintained. Even if a certain cross-sector harmonisation of identification of thresholds may be achieved, the overall identification system would remain complex and would not be expected to lead to a notable increase of identified OESs. Therefore, in this option, it is expected for competent authorities to supervise the same or a similar number of operators as the ones that are currently identified as OES rather than the total number of companies in the respective sectors and subsectors featured in the tables and supporting data below.

For all the data sourced Eurostat (notably number of companies, including medium and large, turnover and average turnover per company), the data used (as the most recent available) is from 2018. Where no source for the data/information is mentioned in the footnotes to the table, it shall be assumed that it is Eurostat data as mentioned above. The table cells marked N/A read as either no available data or not of application for that particular segment.

In relation to the following operators and service providers considered for the addition to the NIS scope due to their digital intensity, inter-dependencies with other sectors and/or importance for society (including in the light of the COVID-19 crisis), insufficient granular data was available to allow a data analysis in this Impact Assessment report: operators of government-owned and privately-owned ground-based infrastructure that support the provision of space-based services; EU reference laboratories (as defined by the Proposal for a Regulation of the European Parliament and of the Council on serious cross-border threats to health); manufacturers of medical devices and in vitro diagnostic medical devices (as defined in Regulation (EU) 2017/745 and Regulation (EU) 2017/746), manufacturers of medical devices considered as critical during a public health emergency (according to Article 20 of the Commission Proposal for a Regulation on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices); entities conducting research and development activities of medicinal products (as defined in Directive 2001/83/EC); electricity market participants as defined by Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined by Directive (EU) 2019/944, and operators of hydrogen production storage and transmission.

**Table 1: Cross-sector summary of the estimation of size and relevant turnover of the sectors, subsectors and types of services currently covered by the NIS framework – policy options 0, 2 and 3**

<i>Sector or type of service</i>	<i>Subsector/s</i>	<i>Number of companies (EU level)</i>	<i>Number of companies of medium and large size (EU level)</i>	<i>Total turnover – million EUR (EU level)</i>	<i>Average turnover per medium and large company – million EUR (EU level)</i>	<i>Number of OES reported by Member States by October 2020 (EU level)</i>	<i>Comments/disclaimers</i>
Energy	Electricity and gas supply	154,967	3,099	1,040,979.37	335.9	872	The data cover also energy generation companies, which are currently not in the NIS scope and are considered under policy options 2 and 3.
Transport <sup>2</sup>	Water	16,051	380	776,749.4	38.22	156	For land transport, the NIS Directive covers only rail (infrastructure managers and railway undertakings) and road (road authorities and operators of intelligent transport services). For the road transport, data was not available to the level of granularity of the types of entities covered by the NIS framework. However, given that the
	Air	4,172	228			165	
	Rail	Approx. 450 <sup>3</sup>	N/A			73	
	Road <sup>4</sup>	N/A	N/A			126	

<sup>2</sup> Of all transport sector, approx. 1.15% are of medium and large size.

<sup>3</sup> Assumption made based on Eurostat data from 2014-2018. No data was available on the medium and large rail enterprises.

<sup>4</sup> The NIS scope (Annex II of the NIS Directive) covers only road authorities and operators of intelligent transport services.

							NIS framework covers entities which are dependent on network and information system, it is unlikely that the number of such road transport entities would be high, rather in the ranges of hundreds.
Banking		6,088 <sup>5</sup>	Approx. 3,500 <sup>6</sup>	Assets of EUR 43,348B <sup>7</sup>	/	411	There was no available data on the overall revenues of banks in the EU.
Financial market infrastructure	CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs	350 <sup>8</sup>	N/A	N/A	N/A	172	There was no available data on the size of the market infrastructures, nor on their revenues.
Health	Hospitals	13,200 <sup>9</sup>	N/A	EUR 475,061.91 (expenditure) <sup>10</sup>	N/A	12,469 <sup>11</sup>	
Drinking	Water	14,116	870	EUR 49,082.8	28	822	These aggregated data are an overestimate,

<sup>5</sup> European Banking Federation data for 2019. It also includes the UK.

<sup>6</sup> Assumption made based using the banks which are covered by the system of European banking supervision as a proxy.

<sup>7</sup> <https://www.ebf.eu/facts-and-figures/statistical-annex/>.

<sup>8</sup> Impact assessment accompanying the review of the European Supervisory Authorities SWD(2017) 308

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

<sup>10</sup> Healthcare expenditure in EU-27 was of EUR 1,309,016.26 million in 2018, while hospitals were the largest providers in expenditure terms, accounting for more than one third (36.3 %) of all expenditure in the EU-27: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare\\_expenditure\\_statistics#Healthcare\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare_expenditure_statistics#Healthcare_expenditure)

<sup>11</sup> Mention should be made that of this total 12,469, 10,897 entities were identified by a single Member State.

water supply and distribution	collection, treatment and supply						since, in addition to water supply, collection and treatment are also covered.
Digital infrastructure	Country-code top-level domain registries	28 major country-code top-level domain (ccTLD) <sup>12</sup>	28	N/A	N/A	173	Very limited market data is available for this sector.
	Individual internet exchange points (IXPs)	140 IXPs <sup>13</sup> (one company usually administers several IXPs)	N/A	N/A	N/A		

<sup>12</sup> one in each Member State plus EURid, which administers .eu

<sup>13</sup> Referenced for 2020. The 140 IXPs are located in the EU, with some being of global importance.



	Domain name system (DNS) providers - made up of a wide range of providers fulfilling different functions along the name resolution chain	Authoritative DNS Resolution	Two root name servers <sup>14</sup> , 28 major ccTLD entities <sup>15</sup> and a large number of domain name registrars and web hosting companies <sup>16</sup>	N/A	N/A		
		Recursive DNS Resolution	DNS resolvers provided by most internet service providers <sup>17</sup> and by third parties, mostly large global technology companies	N/A	N/A	N/A	

<sup>14</sup> providing authoritative DNS resolution for the root zone, located in the Netherlands and Sweden.

<sup>15</sup> The ccTLDs of the 27 Member States (such as .de, .fr or .pl) and of the European Union (.eu), but not counting regional ccTLDs, such as .ax of Åland Islands (Finland). These provide authoritative DNS resolution for their respective TLD namespaces.

<sup>16</sup> offering authoritative DNS resolution as part of their domain registration services.

<sup>17</sup> As part of the internet access arrangement. See the data on electronic communication networks and services.

			located outside the EU.				
Cloud computing services		Estimates of approx. 1,700 <sup>18</sup>	Only few large companies <sup>19</sup> : Amazon <sup>20</sup> , Microsoft, Google and IBM. <sup>21</sup> OVH (the largest European Cloud Service Provider) gets less than 1% of total revenues generated in this market.	N/A	N/A	N/A	<p>According to the 2020 Digital Economy and Society Index (DESI)<sup>23</sup>, in 2018, 26% of European enterprises purchased cloud computing services and incorporated cloud technologies. Among the enterprises that used cloud computing services, 55 % were 'highly dependent'.<sup>24</sup></p> <p>Telecoms are also often heavily featured in their local markets (e.g. Deutsche Telekom, Orange, KPN are among the main cloud providers).<sup>25</sup></p> <p>According to DESI<sup>26</sup>, across the EU market, total revenues generated by public cloud services increased by 21% between 2018 and 2019 and are expected to continue to grow</p>

<sup>18</sup> There is no precise estimate of the number of European cloud service providers, only estimates such as this one by business information platforms: <https://www.crunchbase.com/hub/europe-cloud-computing-companies>

<sup>19</sup> Oligopolistic market.

<sup>20</sup> France, Germany, the UK and the Netherlands.

<sup>21</sup> Salesforce, Rackspace and Oracle are global providers that are further down in the country rankings, with Salesforce ranking fifth overall across Europe.

<sup>22</sup> European players such as OVH, Enter, Aruba, Outscale and Fabasoft do not grasp any significant market shares globally.

<sup>23</sup> <https://ec.europa.eu/digital-single-market/en/integration-digital-technology> .

<sup>24</sup> At the two extremes, the majority of enterprises in the manufacturing sector (51 %) belonged to the upper-medium dependence group, while the majority in information and communication (71 %) reported using advanced services and hence belonged to the high dependence group.

<sup>25</sup> Among European telecoms, Deutsche Telekom is the largest cloud provider thanks to a strong position in Germany and smaller operations in multiple other countries, which help it to place sixth overall across all of Europe. Source: <https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries>

<sup>26</sup> <https://ec.europa.eu/digital-single-market/en/integration-digital-technology>

							by 50% until 2021.
Online marketplaces		7,000 <sup>27</sup>	120 <sup>28</sup>	357,203 <sup>29</sup>	N/A	N/A	By mid-2020, 1 million EU businesses were selling goods and services via online platforms. <sup>30</sup> In 2018, 40 % of EU enterprises with web sales used an e-commerce marketplace. <sup>31</sup> The number of users in e-commerce is expected to amount to 557.5m by 2024. The size of marketplaces varies widely, from turnover exceeding EUR 1 billion to a turnover of less than EUR 100,000. <sup>32</sup>
Online search engines		N/A	One dominant player (Google <sup>33</sup> ), followed by	N/A	N/A	N/A	

<sup>27</sup> Commission estimate of 2019: [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_1168](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168)

<sup>28</sup> Conservative estimate based on a sample of marketplaces for a competition-related sector inquiry conducted by the Commission in 2015-2017: REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report on the E-commerce Sector Inquiry, COM(2017) 229 final and SWD(2017) 154 final: [https://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_sw\\_d\\_en.pdf](https://ec.europa.eu/competition/antitrust/sector_inquiry_sw_d_en.pdf)

<sup>29</sup> Estimate of the revenue in the e-commerce market in Europe in 2020: <https://www.statista.com/outlook/243/102/ecommerce/europe>

<sup>30</sup> For 2017, the European Business-to-Consumer e-commerce turnover was forecasted to reach around EUR 602B, at a growth rate of nearly 14%.

<sup>31</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce\\_statistics#Web\\_sales\\_dominant\\_in\\_all\\_EU\\_countries](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics#Web_sales_dominant_in_all_EU_countries)

<sup>32</sup> REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report on the E-commerce Sector Inquiry, COM(2017) 229 final and SWD(2017) 154 final: [https://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_sw\\_d\\_en.pdf](https://ec.europa.eu/competition/antitrust/sector_inquiry_sw_d_en.pdf)

<sup>33</sup> Over 90% of the general search market in Europe.

			few small players <sup>34</sup>				
--	--	--	------------------------------------	--	--	--	--

---

<sup>34</sup> In the general search market in Europe, Google is the super dominant search engine with an estimated market share of over 90% of web searches (Netmarketshare.com.), followed by Bing with less than 3%. Players such as Seznam in Czechia and Qwant in France are among the very few European-based search engines present on this market.

**Table 2: Cross-sector summary of the estimation of size and relevant turnover for the additional sectors, subsectors and types of services considered for the extension of the NIS scope in policy options 2 and 3**

<i>Sector or type of service</i>	<i>Subsector/s</i>	<i>Number of companies (EU level)</i>	<i>Number of companies of medium and large size (EU level)</i>	<i>Total turnover – million EUR (EU level)</i>	<i>Average turnover per medium and large company – million EUR (EU level)</i>	<i>Comments/disclaimers</i>
Providers of electronic communications networks or of publicly available electronic communications services <sup>3536</sup>	Telecom providers	37,204	N/A	322,297	8.66 (for all sizes)	Both options 2 and 3 would cover all entities, irrespective of the size. For option 3, this represents an exemption from the size cap rule, due to the fact that this highly regulated sector already implements a high level of security standards and excluding micro and small providers from the NIS scope may negatively impact these existing standards.
	Programming and broadcaster providers	7,775	N/A	61,521.9	7.9 (for all sizes)	

<sup>35</sup> Broadcasting services are also considered under this sector, as well as emergency communication services

<sup>36</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information\\_and\\_communication\\_service\\_statistics\\_-\\_NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information_and_communication_service_statistics_-_NACE_Rev._2)

Chemicals and chemical products	Manufacturing	23,845	3,193	555,865.8	135.85	
Waste management	Waste collection, treatment and disposal activities	44,189	2,616	161,537.3	41.76	
Waste water	Sewerage	10,955	473	22,963.9	23	
Postal and courier services	N/A	89,480	869	102,036.2	69.87	
Food supply	Wholesale and retail sale of foods and beverages	595,233	5,303	1,056,828.1	98	The data represent an overestimate, since they also cover wholesale and retail of tobacco, which would not be included in the NIS scope in policy options 2 and 3.
Energy	Electricity generation	3,944 (representing at least 95% of the national net electricity generation in the EU)	82 main electricity generating companies <sup>37</sup>	N/A	N/A	The NIS Directive does not cover electricity generation under the electricity subsector. Policy options 2 and 3 would add this subsector to the NIS scope. The data on electricity generation companies (number and turnover) was included in the above aggregated data covering the

<sup>37</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity\\_generation\\_statistics\\_%E2%80%93\\_first\\_results#Production\\_of\\_electricity](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_generation_statistics_%E2%80%93_first_results#Production_of_electricity)

						electricity and gas subsectors. There was no granular data available on number of medium and large electricity generation companies. By October 2020, Member States (EU-27) have notified to the Commission that they identified 473 OES in the electricity subsector, excluding electricity generation.
	Central oil stocktaking <sup>38</sup>	23	N/A	N/A	N/A	Emergency oil stocks can be held by the Member State itself or through so-called Central Stockholding Entities (CSEs); the Member State may also impose an obligation on economic operators (typically oil companies) to hold the stocks for the benefit of the State. Several Member States have opted for a mixed system where part of the stocks is held by economic operators while the other part is held by a Central Stockholding Entity.  Four Member States currently have no CSE, placing the entire obligation on the industry.
	(Nominated) electricity market	13	N/A	N/A	N/A	Some Member States have/used to have only one NEMO. NEMOs are often small companies.

<sup>38</sup> As defined in point (f) of Article 2 Directive 2009/119/EC

	operators (NEMOs)					
	Electricity market participants	N/A	N/A	N/A	N/A	<p>The inclusion in the NIS scope of electricity market participants, as defined in point (25) of Article 2 of Regulation (EU) 2019/943, providing aggregation, demand response or energy storage services as defined in points (18), (20) and (59) of Article 2 of Directive (EU) 2019/944 providing aggregation, demand response or energy storage services was considered notably due to their importance for the energy sector and the Green Deal.</p> <p>No relevant granular data was available.</p>
	Operators of hydrogen production storage and transmission	N/A	N/A	N/A	N/A	<p>The strategic vision for a climate-neutral EU envisages hydrogen as an important contributor to the EU energy mix by 2050 with a share of 13-14%. This position has been further fostered by the Communication “<i>A hydrogen strategy for a climate-neutral Europe</i>” COM(2020) 301). Turning clean hydrogen into a viable solution to a decarbonised EU will necessarily demand a dedicated infrastructure of key importance for the new EU energy</p>



						system and economy in general.  No relevant granular data was available.
Heat production and supply	District heating and cooling	N/A	N/A	672,000 (823,000 when biofuels and geothermal sectors are included) <sup>39</sup>	N/A	Heating and cooling accounts for approx. 46% of Europe's final energy demand. <sup>40</sup> In EU households, heating and hot water alone account for 79% of total final energy use. <sup>41</sup> Cooling is a fairly small share of total final energy use. In industry, 70.6% of energy consumption is used for space and industrial process heating, 26.7% for lighting and electrical processes such as machine motors, and 2.7% for cooling.
Health	EU reference laboratories	N/A	N/A	N/A	N/A	EU reference laboratories as defined in Article 15 of the Proposal for a Regulation of the European Parliament and of the Council on serious cross-border threats to health and repealing Decision No 1082/2013/EU.  No relevant granular data was available.

<sup>39</sup> considering biomass, biogas, heat pumps and solar-thermal segments.

<sup>40</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity and heat statistics&oldid=493775#Derived heat production](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_and_heat_statistics&oldid=493775#Derived_heat_production)

<sup>41</sup> [https://ec.europa.eu/energy/topics/energy-efficiency/heating-and-cooling\\_en?redir=1](https://ec.europa.eu/energy/topics/energy-efficiency/heating-and-cooling_en?redir=1)

	Research and development activities of medicinal products	N/A	N/A	N/A	N/A	<p>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.</p> <p>No relevant granular data was available.</p>
Manufacturing	Food products	192,328	10,215	724,116.3	57.50	<p>Given the breadth of the manufacturing sector, policy options 2 and 3 would consider the addition only of a number of manufacturing subsectors which would be of greater importance for the society and economies, taking also account of their relevance for the population and for the essential services currently covered by the NIS scope or considered to be added.</p>
	Beverages	27,909	1,047	144,034.1	83.8	
	Basic pharmaceutical products and pharmaceutical preparations	3,352	934	240,420.3	224.46	<p>This includes, among others, the manufacture of medicinal active substances to be used for their pharmacological properties in the manufacture of medicaments: antibiotics, basic vitamins, salicylic and O-acetylsalicylic acids, processing</p>

						of blood, etc and manufacture of medicaments: antisera and other blood fractions, vaccines, etc., manufacture of medical diagnostic preparations, manufacture of radioactive in-vivo diagnostic substances - manufacture of biotech pharmaceuticals.
	Medical devices, and in vitro diagnostic medical devices	N/A	N/A	N/A	N/A	Medical devices as defined in point 1 of Parliament and of the Council on medical devices and in vitro medical diagnostic Article 2 of Regulation 2017/745 of the European devices as defined in point 2 of Article 2 of Regulation 2017/746 of the European Parliament and of the Council.  No relevant granular data was available.
	Medical devices considered as critical during a public health emergency	N/A	N/A	N/A	N/A	The list of public health emergency critical medical devices would be adopted by the Medical Devices Steering Group in line with 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.  No relevant granular data was

						available.
	Computer, electronic and optical products	33,063	2,410	279,521.2	104.2	
	Electrical equipment	38,919	3,378	292,423.3	88.5	
	Machinery and equipment	77,627	8,956	722,795.9	70.1	
	Motor vehicles, trailers and semi-trailers <sup>42</sup>	16,585	2,944	1,106,882.1	369.85	
	Other transport equipment	13,068	1,058	236,726.7	210.65	
Digital infrastructure	Data centres	Geographically concentrated market in Europe with	Market players, such as Equinix or Interxion,	N/A	N/A	Data centres provide different types of services enabling data processing and storage (such as colocation or dedicated hosting). Some large companies also operate their own data

<sup>42</sup> Very specific aspects relating to the manufacturing process of cars are also covered by the General Safety Regulation, notably reflecting the UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles. However, not all cybersecurity risks concerning the manufacturers are covered in that context, nor specific NIS-related requirements, such as incident reporting, information sharing, etc.

		Frankfurt, London, Amsterdam and Paris <sup>43</sup> dominating.	include global companies, but also medium and large firms focusing on the European market.			centres. Data centres are the physical infrastructure used for the provision of cloud-based services. The market is set to reach a size of approx. EUR 36.40 billion by 2025.
	Content delivery networks (CDN)	Highly concentrated global market. None of the major providers are headquartered in the EU.	In 2016, 95 % of global CDN traffic for web-based apps was delivered by 10 companies.	N/A	N/A	N/A
Social networks		Very few social networks providers in Europe, the most significant ones being non-European	Facebook had a market share in social media of over 70% and at times over 80% in 2019-2020, followed by	N/A	N/A	According to DESI <sup>45</sup> , 65% of internet users in the EU used social networks in 2019.

<sup>43</sup> So-called FLAP.

<sup>45</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Social\\_media\\_-\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_-_statistics_on_the_use_by_enterprises)

		businesses.	Pinterest, Twitter and Instagram with less than 12% and other players such as Youtube, Tumblr, Vkontakte with less than 1%. <sup>44</sup>			
Trust service providers		190 active qualified trust service providers <sup>46</sup> operating in 28 of the 31 EU and EEA/EFTA countries <sup>47</sup>	N/A	N/A	N/A	For this types of services, both options 2 and 3 would cover all entities, irrespective of the size. For option 3, this represents an exemption from the size cap rule, due to the fact that within the eIDAS framework, some security standards are already implemented and excluding micro and small providers from the NIS scope may negatively impact these existing standards.
Operators of government-owned and		N/A	N/A	N/A	N/A	Specific ground-based infrastructure that directly supports space-based components of the EU's space

<sup>44</sup> <https://gs.statcounter.com/social-media-stats/all/europe>

<sup>46</sup> There are further 19 trust service providers currently being taken over and further 59 without active trust services listed on the browser that comprise both the qualified and non-qualified status. D.4 – Draft Final Report, 14 September 2020 - *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation)*, SMART 2019/0046, Ecorys, VVA, Deloitte, Spark, pages 21-22 and 24.

<sup>47</sup> The European List of Trusted Lists (LOTL), sourced from the Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020.

privately-owned ground-based infrastructure that support the provision of space-based services						<p>programme, including Galileo, EGNOS, Copernicus, GOVSATCOM and Space Surveillance and Tracking are excluded.</p> <p>No relevant granular data was available.</p>
--	--	--	--	--	--	---

Table 1 above is based on the following data and analysis.

### Energy

In the energy sector, the NIS Directive is currently covering:

- Electricity supply operators
- Electricity Transmission and Distribution System Operators
- Operators of oil transmission pipeline
- Operators of oil production, refining and treatment facilities, storage and transmission
- Gas supply operators
- Gas Transmission and Distribution System Operators
- Gas storage system operators
- LNG system operators
- Natural gas operators
- Operators of natural gas refining and treatment facilities

The data presented below covers the electric power generation, transmission and distribution subsector (*electricity supply subsector*), the manufacture of gas; distribution of gaseous fuels through mains subsector (*gas supply subsector*), as well as steam and air conditioning supply.<sup>48</sup> This data is presented in an aggregated form in Eurostat analysis. Although it does not fully match the scope of the entities covered by NIS under energy sector, it offer a meaningful proxy for the companies operating in the electricity and gas subsectors, which are covered by NIS. Of the above-mentioned aggregated data at EU level, steam and air conditioning supply represents only 5.15% of the number of companies and 2.52% of the overall turnover, which was then deducted from the total number of companies affected and corresponding turnover thereof.

Mention should be made that these aggregate data cover also energy generation companies, which are currently not covered by NIS and which are considered for the extension of the NIS scope under the policy options 2 and 3. The data is therefore an overestimate in this regard for the baseline scenario. Separate data only on electricity generation are presented under options 2 and 3 and the difference highlighted accordingly. There is no EU-wide Eurostat data available on the operators of oil transmission pipelines, oil production, refining and treatment facilities, storage and transmission.

According to the aggregate Eurostat data at EU level, the number of medium and large-size companies represent about 2% of the total number of companies in this sector.

---

<sup>48</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity, gas, steam and air conditioning supply statistics - NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity,_gas,_steam_and_air_conditioning_supply_statistics_-_NACE_Rev._2)



Overview of number of affected businesses in the electricity and gas sector

	<i>Number of companies in electricity, gas, steam and air conditioning supply (2018)</i>	<i>Number of medium and large-size companies in electricity, gas, steam and air conditioning supply (2018)</i>
EU-27	163,125	1,492
<i>EU-27 total extrapolating data on number of medium and large size companies to deduct missing data from some MS<sup>49</sup></i>	/	3,262
<i>EU-27 total only electricity and gas (excluding the steam and air conditioning supply)</i>	154,967	3,099

Source: Eurostat<sup>50</sup>

By October 2020, Member States (EU-27) have notified to the Commission that they identified 872 OES in the energy sector.

The table below reflects the total turnover at EU level of companies in the electricity and gas subsectors in 2018:

*Estimation of average company turnover*

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL only electricity and gas for medium and large size enterprises (excluding the steam and air conditioning supply) (2018)</i>	<i>EU-27 TOTAL only electricity and gas for medium size enterprises (excluding the steam and air conditioning supply) (2018)</i>

<sup>49</sup> Taking account that overall, according to Eurostat data, approximately 2% of the total companies in electricity, gas, steam and air conditioning are of medium and large size.

<sup>50</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity, gas, steam and air conditioning supply statistics - NACE Rev. 2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity,_gas,_steam_and_air_conditioning_supply_statistics_-_NACE_Rev._2).

Turnover (million EUR)	1,450,460.3	1,067,890.2	1,040,979.37	137,890
Number of companies	163,125	3,262	3,099	974
Average turnover per company (million EUR)	/	/	335.9	141,57

Source: Eurostat<sup>51</sup>

### Transport

In the transport sector, the NIS Directive is currently covering:

- Air transport (air carriers, airport managing bodies, airports, entities operating ancillary installations contained within airports, traffic management control operators providing air traffic control).
- Rail transport (infrastructure managers, railway undertakings).
- Water transport (inland, sea and costal passenger and freight water transport companies, managing bodies of ports, operators of vessel traffic services).
- Road transport (road authorities, operators of intelligent transport systems).

*Overview of the number of companies, turnover and average turnover per company for land (rail, road) and transport via pipelines, water and air transport*

	<i>EU-27 TOTAL (2018) – land (rail, road) and transport via pipelines</i>	<i>EU-27 TOTAL for medium and large companies (2018) – land (rail, road) and transport via pipelines</i>	<i>EU-27 TOTAL (2018) – water</i>	<i>EU-27 TOTAL for medium and large companies (2018) – water</i>	<i>EU-27 TOTAL (2018) – air transport</i>	<i>EU-27 TOTAL for medium and large companies (2018) – air transport</i>	<i>EU-27 TOTAL (2018) – land, transport via pipelines, water and air</i>	<i>EU-27 TOTAL for medium and large companies (2018) – land, transport via pipelines water and air</i>
Turnover (million EUR)	548,085.4	304,630	122,979.1	45,046.5	105,684.9	46,592.3 (of which 8.089,2 for medium companies)	776,749.4	396,268.8
Number of companies	880,426	9,760	16,051	380	4,172	228 (of which 149 medium companies)	900,649	10,368
Average turnover per company	/	31.21	/	118.54	/	204.35 (of which 54,28 for medium companies)	/	38.22

<sup>51</sup> Idem.

(million EUR)								
---------------	--	--	--	--	--	--	--	--

Source: Eurostat<sup>52</sup>

The land transport category covered by the above table represents however an aggregate of a wide range of transport companies, ranging from rail to trucking industry, many of which are not actually covered by the NIS Directive, which in relation to land transport covers only: rail transport (in particular infrastructure managers and railway undertakings) and road (in particular road authorities, not covered by the land transport data, and operators of intelligent transport services, in relation to which it is unclear whether they are covered by the overall land transport data). The most recent and comprehensive data on the number of railway operators available in Eurostat dates from 2014: 435 operators. For the following years up to 2018, more data is missing per Member State, but nevertheless one could estimate, taking account of an average increase in the number of companies per Member State between 2014 and 2018, that the overall number of railway operators in 2018 in all Member States would be of about 450.<sup>53</sup> The number of medium and large operators would therefore be smaller. No data was available on the medium and large rail enterprises.

For the road transport, data by Eurostat or from other source was not available to the level of granularity of the types of entities covered by the NIS framework. However, given that the NIS framework covers entities which are dependent on network and information system, it is unlikely that the number of such road transport entities as defined by NIS would be high, rather in the ranges of hundreds, notably as regards medium and large entities.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 620 OES in the transport sector, of which 165 in the air transport, 156 in the water transport and 199 in land transport (73 rail and 126 road).

### Banking

European Banking Federation data shows that there were 6,088 banks in the EU (including UK) in 2019, with assets amounting to EUR 43,348B.<sup>54</sup> In the system of European banking supervision, banks are supervised by the European Central Bank and the national supervisors of the countries that participate in the system.<sup>55</sup> The banking supervision system covers 21 countries (of which four non-EU), 115 significant banks (representing 82% of euro area banking assets), under direct supervision of the European Central Bank, and 2,611 less significant banks, under direct national supervision. The significant and less significant banks covered by the European banking supervision system and amounting to 2,726, could be considered a proxy for medium and large size banks. While the European banking supervision system does not cover all EU Member States, it nevertheless covers a significant number thereof and information could be extrapolated as to assume that approximately 3,500 of credit institutions in the whole of the EU would be of medium and large size.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 411 OES in the banking sector.

<sup>52</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<sup>53</sup> [https://ec.europa.eu/eurostat/databrowser/view/rail\\_ec\\_ent/default/table?lang=en](https://ec.europa.eu/eurostat/databrowser/view/rail_ec_ent/default/table?lang=en)

<sup>54</sup> <https://www.ebf.eu/facts-and-figures/statistical-annex/>

<sup>55</sup> <https://www.bankingsupervision.europa.eu/about/ssmexplained/html/ssm.en.html>

There was no available data on the overall revenues of banks in the EU.

### Financial market infrastructures

The NIS Directive currently covers operators of trading venues and Central Counterparties.

The impact assessment accompanying the review of the European Supervisory Authorities<sup>56</sup> estimated around 350 market infrastructures (such as CCPs, stock exchanges, systemic internalisers, trade repositories and MTFs) in the EU.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 172 OES in the financial market infrastructures.

There was no available data on the size of the market infrastructures, nor on their revenues.

### Health

The NIS Directive currently covers health care settings, including hospitals and private clinics.

Healthcare expenditure in EU-27 was of EUR 1,309,016.26 million in 2018.<sup>57</sup> Hospitals were the largest providers of healthcare in expenditure terms, accounting for more than one third (36.3 %) of all expenditure in the EU-27, i.e. EUR 475.061,91 million. Relative to population size and in euro terms, in 2017 the healthcare expenditure was highest among the EU Member States in Sweden (EUR 5,200 per inhabitant), Denmark and Luxembourg (both EUR 5,100 per inhabitant), with the lowest in Bulgaria (EUR 591 per inhabitant) and Romania (EUR 494 per inhabitant).<sup>58</sup>

There were 2.6 hospitals for 100,000 inhabitants estimated in Europe in 2015, i.e. approximately 13,200.<sup>59</sup>

By October 2020, Member States (EU-27) have notified to the Commission that they identified 12,469 OES in the health sector. The total number of hospitals cannot however be compared with the number of currently identified OES in the healthcare system (i.e.12,469). This is because about 87% of the number of identified OESs comes from the same Member State which identified every single hospital in the country, no matter the size, thus illustrating once more the deep divergence in the identification approaches at Member State level. In option 3, with the application of the size cap, this number is expected to considerably decrease. At the same time, additional medium and large hospitals in other Member States that currently were not identified as OES would be added in the NIS scope. The overall resulting number is however expected to be lower than the couple of thousand ranges.

### Drinking water supply and distribution

The NIS Directive currently covers suppliers and distributors of water intended for human consumption.

---

<sup>56</sup> SWD(2017) 308.

<sup>57</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare\\_expenditure\\_statistics#Healthcare\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Healthcare_expenditure_statistics#Healthcare_expenditure)

<sup>58</sup> Providers of ambulatory health care (25.6 %) and retailers and other providers of medical goods (17.6 %) were the second and third largest providers of healthcare in expenditure terms.

<sup>59</sup> <https://hospitalhealthcare.com/latest-issue-2018/hope-2018/hospitals-in-europe-healthcare-data-9/>

*Overview of the number of companies, turnover and average turnover per company for water collection, treatment and supply*

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>
Turnover (million EUR)	49,082.8	8,861.6	24,374.6
Number of companies	14,116	680	870
Average turnover per company (million EUR)	/	13	28

Source: Eurostat<sup>60</sup>

The above data is wider than the water supply subsector covered by the NIS Directive, therefore the overall number of companies and turnover would be a substantial overestimate.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 822 OES in the drinking water supply and distribution sector.

*Digital infrastructure*

As the NACE classification does not include separate categories for the various digital infrastructures covered by the NIS Directive and considered in the impact assessment, only very limited market data is available for this sector.

➤ *Country-code top-level domain registries*

In 2019 there were 28 major country-code top-level domain (ccTLD) registries with headquarters in the EU (one in each Member State plus EURid, which administers .eu). In 2019, all 28 entities were of medium or small size.

➤ *Internet exchange points*

In 2020 there were 140 individual internet exchange points (IXP) located in the European Union, with some being of global importance. The actual number of companies active in the sector is smaller, as companies often administer more than one IXP. While a small percentage of IXPs is managed by medium-sized companies, most IXPs in the EU are managed by small companies.

➤ *Domain name system providers*

The domain name system (DNS) is made up of a wide range of providers fulfilling different functions along the name resolution chain:

Authoritative DNS resolution:

- There are two root name servers, providing authoritative DNS resolution for the root zone, located in the Netherlands and Sweden.

<sup>60</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

- There are 28 major ccTLD entities<sup>61</sup> providing authoritative DNS resolution for their respective TLD namespaces.
- There is a large number of domain name registrars and web hosting companies offering authoritative DNS resolution as part of their domain registration services. These companies range from micro to large in size and many are located outside the European Union. For example, EURid lists 706 registrars for the .eu domain, of which 116 are located outside the EU.

Recursive DNS resolution:

- DNS resolvers provided by most internet service providers as part of the internet access arrangement (for numbers see section on electronic communication networks and services)
- DNS resolvers provided by third parties, mostly large global technology companies located outside the European Union.

By October 2020, Member States (EU-27) have notified to the Commission that they identified 173 OES in the digital infrastructure sector.

### Cloud computing services

In 2018, the global cloud market<sup>62</sup> was estimated to account for USD 288B and is forecasted to grow by over 1.7 fold by 2021 to reach USD 475B<sup>63</sup>. While *public cloud* is and will remain the largest segment of the global cloud market with estimated revenues of USD 170B in 2018 and USD 277B by 2021, hybrid and private cloud will also grow. Total *hybrid cloud* revenues were estimated<sup>64</sup> to reach USD 52.2 B in 2018. By 2021, total revenues are expected to reach USD 79.5B. In 2018, total *private cloud* revenues were estimated<sup>65</sup> to reach USD 66.5B. By 2021, total private cloud revenues are expected to reach USD 99.9B. ‘*Software as a Service*’ (SaaS)<sup>66</sup> captures the two third of public cloud revenues while ‘*Infrastructure as a service*’ (IaaS)<sup>67</sup> and ‘*Platform as a Service*’ (PaaS)<sup>68</sup> respectively one fifth and one sixth. By 2021, SaaS will continue to capture more than half of the revenues, while IaaS and PaaS will double their respective revenues in average.

The public cloud market structure is oligopolistic composed of only few large companies in which the three leaders - AWS, Microsoft and Google - in aggregate account for

---

<sup>61</sup> The ccTLDs of the 27 Member States and .eu, but not counting regional ccTLDs, such as .ax of Åland Islands (Finland)

<sup>62</sup> Market growth estimations are based on revenues generated from cloud delivery models – public, private and hybrid – for cloud service providers and IT operators.

<sup>63</sup> *Worldwide Whole Cloud Forecast, 2017 – 2021*, IDC, 2017.

<sup>64</sup> ‘*Worldwide Whole Cloud Forecast, 2017 - 2021*, IDC, 2017.

<sup>65</sup> ‘*Worldwide Whole Cloud Forecast, 2017 - 2021*, IDC, 2017.

<sup>66</sup> instant computing infrastructure, provisioned and managed over the internet Examples: Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting.

<sup>67</sup> cloud computing model that provides virtualized computing resources over the internet. Examples: DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE).

<sup>68</sup> cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its own infrastructure. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift.

almost 65% of the market in 2018<sup>69</sup>. AWS is the leader. Alone it accounts for 40% of the public cloud market revenues when estimated by public IaaS and PaaS revenues. Microsoft and Google respectively rank second and third. Alibaba is the main key new entrant with already a strong presence in Asia.

Amazon remains the top cloud provider in Europe and the leader in all major European cloud country markets.<sup>70</sup> Microsoft ranks second, Google third and IBM fourth.<sup>71</sup> European players such as OVH, Enter, Aruba, Outscale and Fabasoft do not grasp any significant market shares globally. At European level, OVH (the largest European Cloud Service Provider) gets less than 1% of total revenues generated in this market. Telcos are often heavily featured in their local markets and Deutsche Telekom, Orange and KPN all rank fourth in their home countries. Among European telecoms, Deutsche Telekom is the largest cloud provider thanks to a strong position in Germany and smaller operations in multiple other countries, which help it to place sixth overall across all of Europe.<sup>72</sup> The table below provides an overview of the cloud services market in Europe for Q1 2020.

### Cloud Services Leadership – Europe

Rank	Total Europe	UK	Germany	France	Netherlands	Rest of Europe
Leader	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft
#3	Google	Google	Google	OVH	Google	Google
#4	IBM	IBM	Deutsche Telekom	Orange	KPN	IBM
#5	Salesforce	Rackspace	IBM	Google	IBM	Salesforce
#6	Deutsche Telekom	Salesforce	Oracle	IBM	Oracle	Swisscom

Based on IaaS, PaaS and hosted private cloud revenues in Q1 2020

Source: Synergy Research Group

While there is no precise estimate of the number of European cloud service providers (some business information platforms estimate over 1,700 cloud service providers in Europe)<sup>73</sup>, as mentioned above, only a handful appear to be of medium and large size and therefore would be under the NIS scope in policy option 3.

Overall, there are two expected future developments in the cloud market. First a significant raise in cloud demand for SaaS solutions that are tailored-made: (i) to respond to sectorial specific companies' needs, (ii) to enable emerging technology services to take-up such as AI and blockchain services and; (iii) to manage energy efficiently and secured data flows and workloads optimization across the entire computing continuum including at the edge. Second, a raise in the demand for both secured hybrid cloud and edge computing solutions associated with increased needs for system integration business products and skills and; change management competences along the computing value

<sup>69</sup> 'No Change at the Top as AWS Remains the Leading Public Cloud Providers in all Regions', Synergy Research Group, 2018.

<sup>70</sup> France, Germany, the UK and the Netherlands.

<sup>71</sup> Salesforce, Rackspace and Oracle are global providers that are further down in the country rankings, with Salesforce ranking fifth overall across Europe.

<sup>72</sup> <https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries>

<sup>73</sup> <https://www.crunchbase.com/hub/europe-cloud-computing-companies>



chain to support companies and public administrations' to successfully transition to hybrid cloud and efficiently utilizing edge computing.

The European cloud infrastructure service revenues (including IaaS, PaaS and hosted private cloud services) were USD 6B in Q1 2020, with trailing twelve-month revenues reaching well over USD 21B. They are currently growing at 38% per year. The four largest country markets are the UK, Germany, France and the Netherlands, which in aggregate account for 63% of the total. Other countries in the top ten are Italy, Spain, Ireland and Belgium. While much smaller than the US market, European cloud revenues are growing more rapidly.<sup>74</sup> Europe's public cloud market is however expected to grow at 22% until 2022.<sup>75</sup>

According to the Digital Economy and Society Index (DESI) thematic report on integration of digital technologies<sup>76</sup>, across the EU market, total revenues generated by public cloud services increased by 21% between 2018 and 2019. Total revenues are expected to continue to grow by 50% between 2019 and 2021. Software security, as a SaaS application, contributed €115.5 million to total SaaS revenues on the EU market. Its revenue growth rate is expected to increase by 48% between 2019 and 2021, making it the fastest growing SaaS application over that period.

### Online marketplaces

By mid-2020, 1 million EU businesses were selling goods and services via online platforms, and more than 50% of SMEs selling through online marketplaces sell cross-border. For 2017, the European Business-to-Consumer e-commerce turnover was forecasted to reach around EUR 602B, at a growth rate of nearly 14%.

Web sales can be carried out via own websites or apps or via e-commerce marketplaces available on external websites or apps. According to Eurostat data, during 2018, 88 % of EU enterprises with web sales used their own websites or apps, while 40 % used an e-commerce marketplace.<sup>77</sup> EU enterprises realised 7 % of their total turnover from web sales during 2018, where 6 % was realised from web sales via own websites or apps and only 1 % from sales via online marketplaces.

At global level, online marketplaces sold USD 2.03 trillion in 2019. Sales on marketplace sites, like those operated by Alibaba, Amazon, eBay and others, accounted for 57% of global web sales in 2019.<sup>78</sup>

According to Statista<sup>79</sup> the revenue in the e-commerce market in Europe is projected to reach USD 421,927m in 2020. The number of users in e-commerce is expected to amount to 557.5m by 2024. The average revenue per user is expected to amount to USD 877.33.

In 2019, the Commission estimated a number of approximately 7,000 marketplaces in the EU.<sup>80</sup> In a sector inquiry into e-commerce launched by the Commission in May 2015 and finalised in June 2017, 37 marketplaces were selected for the inquiry, including the most important marketplaces and price comparison tools in the EU at the time, both the biggest

---

<sup>74</sup> <https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries>

<sup>75</sup> International Data Corporation (IDC).

<sup>76</sup> <https://ec.europa.eu/digital-single-market/en/integration-digital-technology>

<sup>77</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce\\_statistics#Web\\_sales\\_dominant\\_in\\_all\\_EU\\_countries](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics#Web_sales_dominant_in_all_EU_countries)

<sup>78</sup> Digital Commerce 360's analysis:

<sup>79</sup> <https://www.statista.com/outlook/243/102/ecommerce/europe>

<sup>80</sup> [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_1168](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168)



international players and the most relevant regional ones, covering the sale and price comparison of all products within the scope of the sector inquiry.<sup>81</sup> The size of marketplaces varies widely and ranges from marketplaces with turnover exceeding EUR 1 billion to marketplaces with a turnover of less than EUR 100,000. The selected marketplaces targeted altogether customers in 14 Member States. It can therefore be considered that a conservative proxy for the number of large and medium online marketplaces active across all Member States could be roughly 120 marketplaces.

### Online search engines

In the general search market in Europe there is one super dominant search engine, Google, with an estimated market share of over 90% of web searches<sup>82</sup>, followed by Bing with less than 3%. European players such as Seznam in Czechia and Qwant in France are among the very few European-based search engines present on this market.

Table 2 above is based on the following data and analysis.

### Providers of electronic communications networks or of publicly available electronic communications services<sup>83</sup>

*Overview of number of telecommunication operators, turnover and average company turnover*

	<i>EU-27 TOTAL (2018)</i>
Turnover (million EUR)	322,297
Number of companies	37,204
Average turnover per company (million EUR)	8.66

Source: Eurostat<sup>84</sup>

*Overview of number of providers of programming and broadcasting activities, turnover and average company turnover*

	<i>EU-27 TOTAL (2018)</i>
Turnover (million EUR)	61,521.9
Number of companies	7,775
Average turnover per company (million EUR)	7.9

Source: Eurostat<sup>85</sup>

<sup>81</sup> REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Final report on the E-commerce Sector Inquiry, COM(2017) 229 final and SWD(2017) 154 final: [https://ec.europa.eu/competition/antitrust/sector\\_inquiry\\_swd\\_en.pdf](https://ec.europa.eu/competition/antitrust/sector_inquiry_swd_en.pdf)

<sup>82</sup> Netmarketshare.com

<sup>83</sup> Broadcasting services and emergency communication services would also be included in this category.

<sup>84</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information\\_and\\_communication\\_service\\_statistics\\_-\\_NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information_and_communication_service_statistics_-_NACE_Rev._2)

### Chemicals (manufacture)

The production of chemicals hazardous to health in the EU was 222.6 million tonnes in 2018.<sup>86</sup> The aggregated production of chemicals hazardous to environment is of about 84 million tonnes.

*Overview of number of providers of manufacturing of chemicals, turnover and average company turnover*

	<i>EU-27 (2018)</i>	<i>TOTAL</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	555,865.8		433,797.5	105.238,9
Number of companies	23,845		3,193	2.422
Average turnover per company (million EUR)			135.85	43,45

Source: Eurostat<sup>87</sup>

### Digital infrastructure – Data centres

Data centres provide different types of services enabling data processing and storage (such as colocation or dedicated hosting). Some large companies also operate their own data centres. Data centres are the physical infrastructure used for the provision of cloud-based services. The European data centre market is geographically concentrated with Frankfurt, London, Amsterdam and Paris (so-called FLAP) dominating. It is set to reach a size of USD 43 billion by 2025. Market players, such as Equinix or Interxion, include global companies but also firms of medium and large size focusing on the European market.

### Digital infrastructure – Content delivery networks

Content delivery networks (CDN) operate on a highly concentrated global market. None of the major providers are headquartered in the European Union. In 2016, 95% of global CDN traffic for web-based apps was delivered by only 10 companies. In 2019, the 10 biggest providers by number of customers were of large size.

### Waste management

*Overview of the number of companies, turnover and average turnover per company for waste collection, treatment and disposal activities; materials recovery*

---

<sup>85</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information\\_and\\_communication\\_service\\_statistics\\_-\\_NACE\\_Rev.\\_2](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Information_and_communication_service_statistics_-_NACE_Rev._2)

<sup>86</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Chemicals\\_production\\_and\\_consumption\\_statistics#Production\\_of\\_chemicals\\_hazardous\\_to\\_the\\_environment](https://ec.europa.eu/eurostat/statistics-explained/index.php/Chemicals_production_and_consumption_statistics#Production_of_chemicals_hazardous_to_the_environment)

<sup>87</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	161,537.3	109,256.4	36.829,5
Number of companies	44,189	2,616	2.152
Average turnover per company (million EUR)	/	41.76	17.11

Source: Eurostat<sup>88</sup>

### Wastewater

Overview of the number of companies, turnover and average turnover per company for the sewerage subsector

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	22,963.9	10,880.7	4.929,3
Number of companies	10,955	473	408
Average turnover per company (million EUR)	/	23	12

Source: Eurostat<sup>89</sup>

### Manufacturing

Other than the manufacturing of chemicals and chemical products, which was also covered separately above, the *manufacturing subsectors considered in policy options 2 and 3 and their respective size and turnover are included in the table below.*

<sup>88</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<sup>89</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<i>Manufacturing subsectors</i>	<i>Number of companies (2018)</i>	<i>Number of companies of medium and large size (2018)</i>	<i>Total turnover – million EUR (2018)</i>	<i>Total turnover for companies of medium and large size – million EUR (2018)</i>	<i>Average turnover per company of medium or large size – million EUR (2018)</i>
Food products	192,328	10,215 (of which 8.149 medium companies)	724,116.3	587,440 (of which 189.078,6 for medium companies)	57.50 (23.2 for medium companies)
Beverages	27,909	1,047 (of which 813 medium companies)	144,034.1	87,748.1 (of which 23,157.2 for medium companies)	83.8 (28.48 for medium companies)
Basic pharmaceutical products and pharmaceutical preparations	3,352	934 (of which 538 medium companies)	240,420.3	209,649.6 (of which 14,802.3 for medium companies)	224.46 (27.51 for medium companies)
Computer, electronic and optical products	33,063	2,410 (of which 1,786 medium companies)	279,521.2	251,145.4 (of which 43.496,5 for medium companies)	104.2 (24.35 for medium companies)
Electrical equipment	38,919	3,378 (of which 2,425 medium companies)	292,423.3	298,973.1 (of which 49,072.7 for medium companies)	88.5 (20.23 for medium companies)
Machinery and equipment	77,627	8,956 (of which 7,053 medium companies)	722,795.9	627,831.8 (of which 145,420.4 for medium companies)	70.1 (20.61 for medium companies)

Motor vehicles, trailers and semi-trailers	16,585	2,944 (of which 1,771 medium companies)	1,106,882.1	1,088,852 (of which 42,646.2 for medium companies)	369.85 (24.08 for medium companies)
Other transport equipment	13,068	1,058 (of which 739 medium companies)	236,726.7	222,876.3 (of which 15.512,3 for medium companies)	210.65 (21 for medium companies)

Source: Eurostat<sup>90</sup>

### Postal and courier services

Overview of the number of companies, turnover and average turnover per company in the postal and courier activities subsectors

	<i>EU-27 TOTAL (2018)</i>	<i>EU-27 TOTAL for medium and large companies (2018)</i>	<i>EU-27 TOTAL for medium companies (2018)</i>
Turnover (million EUR)	102,036.2	60,717.9	3,238
Number of companies	89,480	869	621
Average turnover per company (million EUR)	/	69.87	5.21

Eurostat<sup>91</sup>

### Food supply

In policy options 2 and 3 food supply would be added to the NIS scope, and in particular the subsectors of wholesale and retail sale of foods and beverages.

Overview of the number of companies, turnover and average turnover per company for wholesale and retail of food, beverages and tobacco

	<i>EU-27 TOTAL (2018) – wholesale</i>	<i>EU-27 TOTAL for medium and large companies (2018) – wholesale</i>	<i>EU-27 TOTAL (2018) – retail</i>	<i>EU-27 TOTAL for medium and large companies (2018) – retail</i>	<i>EU-27 TOTAL (2018) – wholesale and retail</i>	<i>EU-27 TOTAL for medium and large companies (2018) – wholesale and retail</i>

<sup>90</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

<sup>91</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do>

Turnover (million EUR)	924,834.3	501,698.5	131,993.8	18,200.6	1,056,828.1	519,900 (of which 217.427,5 for medium companies)
Number of companies	188,146	4,352	407.087	951	595,233	5,303 (of which 4,593 medium)
Average turnover per company (million EUR)	/	115.27	/	19.14	/	98 (47.33 for medium companies)

Source: Eurostat<sup>92</sup>

The above data represent an overestimate since they also cover wholesale and retail of tobacco, which would not be included under NIS scope in policy options 2 and 3.

New energy subsectors and/or operators

- *Electricity generation*

The data on electricity generation companies (number and turnover) was included in the above aggregated data covering the electricity and gas subsectors.

In 2018, there were 3,944 generating companies representing at least 95% of the national net electricity generation in the EU and 82 main electricity generating companies.<sup>93</sup>

By October 2020, Member States (EU-27) have notified to the Commission that they identified 473 OES in the electricity subsector, excluding electricity generation. There was no granular data available on number of medium and large electricity generation companies.

- *Central oil stockholding entities*

Under the Oil Stocks Directive (2009/119/EC), Member States must maintain emergency stocks of crude oil and/or petroleum products equal to at least 90 days of net imports or 61 days of consumption, whichever is higher. Member States may meet this stockholding obligation in different ways. Emergency stocks can be held by the Member State itself or through so-called Central Stockholding Entities (CSEs) set up for this purpose in the form of a non-profit making body or service; the Member State may also impose an obligation on economic operators (typically oil companies) to hold the stocks for the benefit of the State. Several Member States have opted for a mixed system where part of the stocks is held by economic operators while the other part is held by a Central Stockholding Entity.

<sup>92</sup> <https://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do/>

<sup>93</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity\\_generation\\_statistics\\_%E2%80%93\\_first\\_results#Production\\_of\\_electricity](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_generation_statistics_%E2%80%93_first_results#Production_of_electricity)

The most centralised systems are those in which one organisation (the CSE usually established by the State), is the sole organisation responsible for holding emergency stocks. The most decentralised model is a model in which the entire stockholding obligation is put on the economic operators in the oil industry (and consequently no CSE exists), while the intermediate model is one in which the stockholding obligation is divided between industry and the CSE.

There are 23 Central Stockholding Entities in the European Union. Four Member States currently have no CSE, placing the entire obligation on the industry: Greece, Malta, Romania and Sweden. Two Member States, albeit having established a CSE, put the obligation almost exclusively on industry: Italy and Luxembourg.

- *(Nominated) Electricity market operator*

A nominated electricity market operator' or 'NEMO' means a market operator designated by the competent authority to carry out tasks related to single day-ahead or single intraday coupling, as defined in point (8) of Article 2 of the Regulation on the internal market for electricity (EU) 2019/943. An 'electricity market operator' means an entity that provides a service whereby the offers to sell electricity are matched with bids to buy electricity, as defined in point (7) of Article 2 of the Regulation on the internal market for electricity (EU) 2019/943.

The energy market highly depends on trading platforms and are thus crucial for the market. These trading platforms rely on IT systems.

There are approx. 16 NEMOs in Europe. Some Member States have/used to have only one NEMO: AT (EXAA); BG (IBEX); Croatia (CROPEX), CZ (OTE); GR (HENEX); HU (HUPX); Ireland (EirGrid); IT (GME); PL (TGE); PT (OMIE); RO (OPCOM); SK (OKTE); SI (BSP);. In other Member States the two main players are EPEX and Nordpool, with also the new entrant Nasdaq present in some of them.

NEMOs are often small companies. EPEX is one of the biggest NEMO and has 200 employees.

- *Electricity market participants engaged in aggregation, demand response or energy storage services*

Electricity market participant engaged in aggregation, demand response or energy storage services means a natural or legal person who is engaged in aggregation or who is an operator of demand response or energy storage services, including through the placing of orders to trade, in one or more electricity markets, including in balancing energy markets, as defined in point (25) of Article 2 of Regulation on the internal market for electricity (EU) 2019/943.<sup>94</sup>

Aggregation, storage and demand response increase the flexibility in energy markets and are highly needed elements, which are evolving very rapidly and will increase in numbers.

These categories of services within the energy sector are developing and are an important part of the implementation of the Green Deal. All these categories of services rely heavily on IT and OT as there is a need to respond to real time signals.

---

<sup>94</sup> this definition refers only to market operators dealing with aggregation, demand response services, energy storage.

### Heat production and supply

There were no granular data available on the number of companies and turnover in the heat production and supply sector in the EU. Some estimates indicate a turnover of the heating and cooling industry (considering biomass, biogas, heat pumps and solar-thermal segments) of EUR 67.2 billion and EUR 82.3 billion when biofuels and geothermal sectors are included.

### Social networks

According to DESI<sup>95</sup>, social networks (51 %) were the most used form of social media platforms in 2019. Furthermore, 65% of internet users in the EU used social networks in 2019.<sup>96</sup> In Europe, the social media platforms players are very few. Facebook had a market share in social media of over 70% and at times over 80% in 2019-2020, followed by Pinterest, Twitter and Instagram with less than 12% and other players such as Youtube, Tumblr, Vkontakte with less than 1%.<sup>97</sup>

### Trust service providers

The European List of Trusted Lists (LOTL) comprises all of the trusted lists managed by Member States within the scope of the Regulation (e.g. eSignatures, eSeals, WA, eTimestamps, ERDs, eSeal creation devices, eSignature creation devices, preservation service/archive). The Trusted List Browser developed by the European Commission<sup>98</sup> covers all trust service providers established in the European Union or in Norway, Liechtenstein or Iceland.

According the LOTL<sup>99</sup>, there are currently 190 active qualified trust service providers operating in 28 of the 31 EU and EEA/EFTA countries. There are a further 19 trust service providers currently being taken over and a further 59 trust service providers without active trust services listed on the browser that comprise of both the qualified and non-qualified status.<sup>100</sup>

The draft final report of the *Evaluation study of the eIDAS Regulation*<sup>101</sup> notes that qualified eSignatures are the services provided most on the market, followed by qualified time stamps and qualified eSeals. Out of the core trust services<sup>102</sup>, the qualified electronic registered delivery service is the most limited one, with 20 active services in seven Member States. The market offering of qualified website authentication certificates is additionally relatively lower than the offering for qualified eSignatures, qualified eSeals and qualified time stamps, which is likely due to the market being highly concentrated<sup>103</sup>.

---

<sup>95</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Social\\_media\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/Social_media_statistics_on_the_use_by_enterprises)

<sup>96</sup> <https://ec.europa.eu/digital-single-market/en/use-internet>

<sup>97</sup> <https://gs.statcounter.com/social-media-stats/all/europe>

<sup>98</sup> <https://webgate.ec.europa.eu/tl-browser/#/>

<sup>99</sup> Sourced from the Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020.

<sup>100</sup> D.4 – Draft Final Report, 14 September 2020 - *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation)*, SMART 2019/0046, Ecorys, VVA, Deloitte, Spark, pages 21-22 and 24.

<sup>101</sup> Idem.

<sup>102</sup> Qualified certificate for electronic signature, Qualified certificate for electronic seal, Qualified time stamp, Qualified certificate for website authentication, Qualified electronic registered delivery service.

<sup>103</sup> ENISA, 2015, Qualified Website Authentication Certificates.



*Preliminary data on number of active qualified trust services in Europe<sup>104</sup>*

Qualified certificate for electronic signature	152	28	AT, BE, BG, HR, CY, CZ, EE, FI, FR, DE, EL, HU, IS, IE, IT, LI, LT, LV, LU, MT, NL, NO, PL, PT, RO, SK, SI, ES
Qualified time stamp	109	23	AT, BE, BG, HR, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified certificate for electronic seal	102	24	AT, BE, BG, HR, CY, CZ, EE, FR, DE, EL, HU, IE, IT, LV, LT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified certificate for website authentication	51	20	AT, BE, BG, HR, CZ, FI, FR, DE, EL, HU, IT, LU, NL, NO, PL, PT, RO, SK, SI, ES
Qualified electronic registered delivery service	20	7	BE, FR, DE, NL, PL, SI, ES
Qualified validation service for qualified electronic signature	15	10	BE, BG, CZ, FR, LT, PL, SI, SK, ES, SE
Qualified validation service for qualified electronic seal	15	10	BE, BG, CZ, FR, LT, PL, SK, SI, ES, SE
Qualified preservation service for qualified electronic seal	13	9	BG, CZ, FR, HU, MT, PL, RO, SK, ES
Qualified preservation service for	12	7	BG, CZ, FR, HU, MT, PL, RO, SK, ES

<sup>104</sup> Statistics sourced from Trusted List Browser (<https://webgate.ec.europa.eu/tl-browser/#/>) on 8 September 2020.

qualified electronic signature			
--------------------------------------	--	--	--

Source: Draft Final Report, 14 September 2020 - Evaluation study of the Regulation no.910/2014 (eIDAS Regulation), SMART 2019/0046, Ecorys, VVA, Deloitte, Spark

Member States may add trust services other than qualified ones to the Trusted List on a voluntary basis.

A study that looked into the uptake of eIDAS services by SMEs found a generally low level of awareness of eIDAS solutions among SMEs: only 17% of SMEs had used an eIDAS solution already in their business.<sup>105</sup>

➤ **Public administration (from the perspective of being included under the NIS scope)**

In policy options 2 and 3, the NIS framework would only cover under ‘public administration’ central governments (i.e. all administrative departments of the state and other central agencies whose responsibilities cover the whole economic territory of a country), as well as the major socio-economic regions (104 in total according to the Nomenclature of territorial units for statistics–NUTS 2021 classification) and the basic regions for the application of regional policies (283 in total according to the NUTS 2021 classification).<sup>106</sup>

No attempt was made however for estimating the number of individual public institutions since the objective of the cost assessment is to make a global estimate of the total cost for the public sector. Data for the public administration relate to the operating costs. ICT spending in the public sector is typically expressed as a percentage of the operating expenditure instead of revenues or turnover.<sup>107</sup>

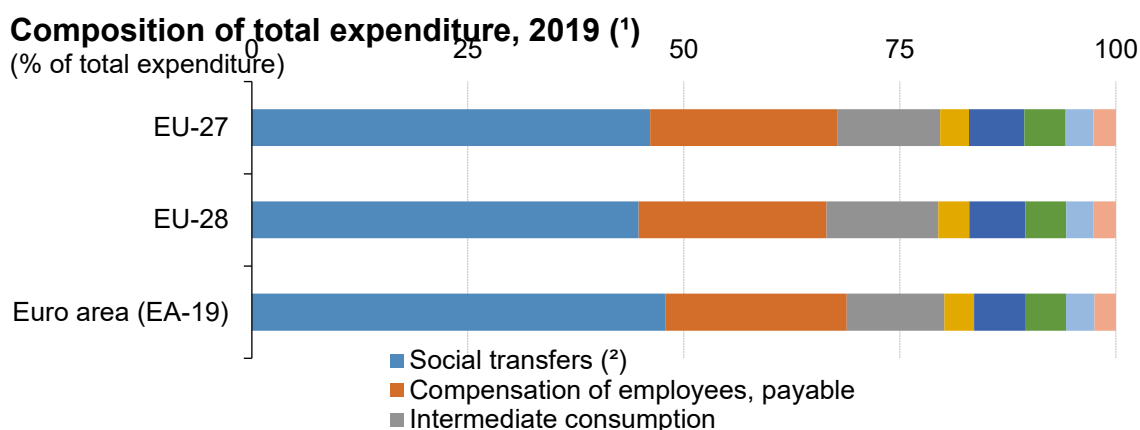
According to Eurostat<sup>108</sup>, in 2019, the total expenditure at **central government** level in the EU-27 was of 22% of GDP. The total revenue was of 21.7% of the GDP. At the **local government** level, the total expenditure was the same as the total revenue: 10.9% of the GDP. The composition of total government expenditure is reflected in the table below:

<sup>105</sup> eIDAS Study on pilots for replication of multipliers: supporting the uptake of eIDAS services by SMEs, SMART 2016/ 0084. See publication here: <https://op.europa.eu/en/publication-detail/-/publication/0627f219-5044-11e9-a8ed-01aa75ed71a1/language-en>.

<sup>106</sup> <https://ec.europa.eu/eurostat/web/regions/background>.

<sup>107</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Total\\_general\\_government\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Total_general_government_expenditure)

<sup>108</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government\\_finance\\_statistics](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_finance_statistics)



<sup>(1)</sup> Data extracted on 22.04.2020.

<sup>(2)</sup> Social benefits other than social transfers in kind and social transfers in kind - purchased market production.

Source: Eurostat (online data code: gov\_10a\_main), Government finance statistics<sup>109</sup>

***Estimating the percentage of ICT security spending out of ICT spending and total revenue and evolution thereof of the sectors, subsectors and types of services currently covered and to be covered by NIS in the preferred option***

There is no available data to measure the actual impact of the NIS Directive on the level of ICT security spending for the companies activating in the sectors and subsectors or providing services under the NIS scope. Given the above-mentioned lacunae in comparable economic data, the analyses of economic impact and efficiency under all policy options, including the baseline scenario, would refer to widely accepted qualitative indicators for assessing the costs and benefits of various cybersecurity measures, along the lines described above, as well as a number of illustrative examples of tools used for this purpose and outcome thereof.

In the Impact Assessment that supported the proposal for the NIS Directive<sup>110</sup>, the level of **investment in IT security** was estimated on the basis of Gartner’s global IT key metrics which indicated a percentage of IT security expenditure per sector out of the total revenue. The global ICT security spending data were estimated for 2012 and ranged between 3.04% to 6.61% of the total ICT spending per sector (with lowest in transport and healthcare, and highest in energy and digital infrastructure, including telecoms), while the ICT spending ranged between 1.10% and 7.60% of the total turnover per sector (with lowest in the energy sector and the highest in the banking and financial sector, as well as digital infrastructure sector and telecoms). One could therefore assume that, at global level, the ICT security spending at the time was in average about 5% of the ICT spending per sector and ICT spending was in average 4.3% of the total turnover, therefore leading to an average ICT security spending of about 0.215% of the total turnover.

The corresponding updated granular data were not available to the Commission at the time of the writing of this impact assessment report. However, while analysing Gartner press releases on their regular forecasts of the percentage of global IT security spending out of the total revenues, one could see the overall evolution of **ICT security spending and ICT spending** over the years. Thus, the estimated increases of ICT security spending

<sup>109</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government\\_finance\\_statistics#Government\\_revenue\\_and\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Government_finance_statistics#Government_revenue_and_expenditure)

<sup>110</sup> SWD(2013) 32 final.

at global level out of ICT spending were from USD 65.9 billion in 2013<sup>111</sup>; to USD 123.8 billion in 2020 (i.e. an average growth of 82.83% from 2013 to 2020)<sup>112</sup>, while the evolution of ICT spending was estimated from USD 2.69 trillion in 2013<sup>113</sup> to USD 3.56 trillion in 2020 (taking account a conservative scenario that assumes a post-COVID-19 recession)<sup>114</sup>, i.e. an increase of 32.34% from 2013 to 2020.

Some sectors or services would indeed have a more significant or faster growth of ICT security investment than others. For example, according to Gartner estimates and forecast, **8 of 10 cybersecurity markets are projected to grow faster than the market average, with cloud security growing the fastest.** Cloud security is the smallest, fastest-growing cybersecurity market segment with market size of USD 439 million in 2019, with a projected growth of 33% growth in 2020 up to USD 585M, mainly due to its small initial market size and organizations' preference for cloud-based cybersecurity solutions.<sup>115</sup>

In the banking sector, a survey by Deloitte and FS-ISAC<sup>116</sup>, referred to in the Impact Assessment for the Digital Resilience Act for financial services<sup>117</sup>, shows that on average banks, insurers, investment management firms and other financial services companies spend between 6% and 14% of their IT budget on cybersecurity, with an average of 10%. These account to a range of between 0.2% and 0.9% of the total revenues, with an average of about 0.3%. The above-mentioned impact assessment stresses that, while it is impossible to estimate the recurring costs of a general improvement of qualitative ICT risk requirements, it could be estimated that bringing ICT requirements up to a decent standard for all financial institutions would mean that institutions which have spending below the average would have to bring this up to the average. Another survey by Deutsche Bank<sup>118</sup> provides a breakdown on how much of the IT spending is dedicated to cyber security by financial institutions. On average, around 10% of financial institutions are below the 6%-14% range mentioned above.

Considering the above-mentioned overall evolution of global ICT spending and ICT security spending, one could assume for the purposes of this impact assessment that the average ICT security spending per sector would be in 2020 of approx. 9.14% of the ICT spending per sector. Depending on the level of cybersecurity maturity and capabilities of the sector, an adjustment of +/-3% could be made to this average. As for the overall ICT spending per sector, the average would be of approx. 5.69% of the total turnover. Depending on the level of digitalisation of the sector, an adjustment of +/-3% could be made to this average. This would entail an ICT security spending of approximately 0.52% of the total turnover. These extrapolations indeed do not reflect the precise differences in ICT and ICT security spending between sectors, which can be considerable, therefore it may be an overestimate for some and an underestimate for some others, however, overall, it may offer a conservative calculation basis which can help estimate to a certain extent

---

<sup>111</sup> <https://www.gartner.com/en/newsroom/press-releases/2014-08-22-gartner-says-worldwide-information-security-spending-will-grow-almost-8-percent-in-2014-as-organizations-become-more-threat-aware>

<sup>112</sup> <https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem>

<sup>113</sup> <https://www.gartner.com/en/documents/2601718>

<sup>114</sup> <https://www.gartner.com/en/documents/3982876>

<sup>115</sup> <https://www.forbes.com/sites/louiscolombus/2020/08/09/cybersecurity-spending-to-reach-123b-in-2020/#766ad2a0705f>.

<sup>116</sup> <https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html>.

<sup>117</sup> SWD(2020) 203 final, p.43.

<sup>118</sup> [https://www.db.com/newsroom\\_news/Deutsche\\_Bank\\_Investor\\_Report.pdf](https://www.db.com/newsroom_news/Deutsche_Bank_Investor_Report.pdf)

the weight of ICT security spending in the turnover of entities covered or considered to be covered in the future by NIS.

The overall global ICT security spending<sup>119</sup> increased with approximately 22% from 2017 (the year after the entry into force of the NIS Directive) and 2020. While this increase is not directly linked to the NIS Directive, one can assume nevertheless that it also integrates the spending generated by security requirements such as those provided by NIS which largely follow international standards. Therefore, assuming that in the medium-term (three to four years), the **new sectors** to be added to the NIS scope would entail **about 22% increase in their ICT security spending** would be a conservative assumption, most likely an overestimate, since it would consider a premise where the only trigger for extra IT security investment in these sectors and services would be the NIS framework. Yet, many other factors would naturally contribute to such increase, such as evolution of technologies and threat landscape, GDPR and other regulatory obligations, effects of particular incidents that may occur in the meantime or major crises, level of awareness, level of digitalisation, etc.

**For the sectors currently covered by the NIS Directive**, one would rather expect a more limited increase of ICT spending in the coming three to four years, slightly over (+4-5%) the pace of ICT security spending increase forecasted by Gartner in December 2019, prior to the COVID-19 crisis: i.e. **about 12% increase**.<sup>120</sup>

## 2. Summary of costs and benefits

The tables below present the costs and benefits which have been identified and analysed during the impact assessment process.

(1) *Estimates are relative to the baseline for the preferred option as a whole (i.e. the impact of individual actions/obligations of the preferred option are aggregated together); (2) The comment section indicates which stakeholder group is the main recipient of the benefit.*

<b><i>I. Overview of Benefits (total for all provisions) – Preferred Option</i></b>		
<b><i>Description</i></b>	<b><i>Amount</i></b>	<b><i>Stakeholder group main recipient of the benefits</i></b>
<b><i>Direct benefits</i></b>		
Reduce administrative burden by discarding the identification process	n/a	<ul style="list-style-type: none"> <li>• national authorities</li> <li>• businesses</li> </ul>
More clarity and further harmonisation would allow more focus on core cybersecurity tasks	n/a	<ul style="list-style-type: none"> <li>• national authorities</li> </ul>
Increase in compliance with security requirements	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>

<sup>119</sup> <https://www.statista.com/statistics/790834/spending-global-security-technology-and-services-market-by-segment/>

<sup>120</sup> <https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem>

		<ul style="list-style-type: none"> <li>• national authorities</li> </ul>
Single entry point for notifications concerning security breaches stemming from the NIS Directive, the General Data Protection Regulation and the ePrivacy Directive reducing administrative burden stemming from reporting obligations	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>
Decrease in cybercrime losses (medium/long term by implementing higher level of security requirements)	Use of higher level of security requirements and in particular fully deployed security automation (e.g. use of advanced technology, AI, automated scanning tools, etc) help companies reduce the lifecycle of a breach by 74 days compared to companies with no security automation deployment, from 308 to 234 days.	<ul style="list-style-type: none"> <li>• businesses</li> <li>• citizens</li> </ul>
Decrease in security incidents and cybercrime losses	Estimated reduction in cost of cyber incidents by EUR 11.3 billion over a 10-year period	<ul style="list-style-type: none"> <li>• businesses</li> <li>• citizens</li> </ul>
Reduction in cost liability for breaches	n/a	<ul style="list-style-type: none"> <li>• businesses</li> <li>• citizens</li> </ul>
Increase of trust of customers	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>
Protection from unfair competition (e.g. by avoiding industrial espionage)	n/a	<ul style="list-style-type: none"> <li>• businesses</li> </ul>
Increased and consistent level of resilience at the level of key businesses and cross-sector	n/a	<ul style="list-style-type: none"> <li>• businesses</li> <li>• national authorities</li> <li>• citizens</li> </ul>
Improved situational awareness	n/a	<ul style="list-style-type: none"> <li>• businesses</li> <li>• national authorities</li> <li>• citizens</li> </ul>

Increased operational capabilities	n/a	<ul style="list-style-type: none"> <li>• national authorities</li> </ul>
<b><i>Indirect benefits</i></b>		
Improved personal data protection	n/a	<ul style="list-style-type: none"> <li>• citizens</li> </ul>

<b>II. Overview of costs – Preferred option</b>							
		Citizens/Consumers		Businesses		Administrations	
		One-off	Recurrent	One-off	Recurrent	One-off	Recurrent
<b>Action (a)</b> <b>Extension of the NIS scope (including adding a size cap)</b>	Direct costs	n/a	n/a	<p><i>Average 22% increase in ICT security spending for the new sectors/services added to the NIS scope in the next 3-4 years.</i></p> <p><i>For the new sectors or services, an increase of about 25% of ICT spending could be expected for medium enterprises.</i></p> <p><i>Note: overall, in addition to the estimated increase in ICT spending triggered by the extension of the sectorial scope, an</i></p>	<p>Costs of implementation of higher security requirements and documented security measures</p>	<p>Personnel and administrative costs leading to an overall increase of approx. 20-30% of resources of the relevant authorities per Member State at central level mainly needed for performing supervisory actions and interactions with industry (including sector-specific)</p>	<p>Regular personnel and enforcement costs</p>



				<p><i>average 12% increase in ICT security spending is estimated for the sectors/services currently under the scope of the NIS Directive scope in the next 3-4 years. For medium enterprises, this estimate is of approx. 15%. This increase concern the cumulative effect of all measures envisaged by the preferred option.</i></p>			
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (b)</b>		n/a	n/a	Negligible personnel costs (notably legal departments), no additional FTE	n/a	n/a	n/a
<i>Discarding the identification process and putting all operators and digital service providers under an equal footing, while</i>	Direct costs						
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a

<i>differentiating on importance/criticality grounds</i>							
<b>Action (c)</b> <i>Further harmonising and streamlining risk management/security requirements</i>	Direct costs	n/a	n/a	<ul style="list-style-type: none"> <li>• Personnel (including potentially setting up new in-house teams): 2 -4 extra FTEs</li> <li>• Administrative costs</li> <li>• Opportunity costs</li> <li>• Potential increase in purchase costs on cybersecurity of +10-15%.</li> </ul>	<ul style="list-style-type: none"> <li>• Purchase costs (consultancy, audit, penetration tests, etc.)</li> </ul>	Approx. 20-30% increase in budget/expenses), same increase as triggered by supervisory and enforcement-related measures + administrative costs for the sector-specific decentralised models for the new sectors/services to be added to the NIS scope	Recurrent personnel and technical costs (audits, testing, etc).
	Indirect costs	Potential slight increase in prices of products as a result of investment in cybersecurity technologies and measures	n/a	n/a	n/a	n/a	n/a

<b>Action (d)</b> <i>Security elements concerning supplier relationships and supplier-specific risk assessment</i>	Direct costs	n/a	n/a	<ul style="list-style-type: none"> <li>• Personnel - in average 1 FTE</li> <li>• Purchase costs (consultancy, audit)</li> <li>• Opportunity costs</li> </ul>	<ul style="list-style-type: none"> <li>• Personnel and potential regular outsourcing for risk assessments (notably for SMEs): potential increase of 2-4% in recurrent purchase ICT security costs</li> </ul>	<ul style="list-style-type: none"> <li>• Part of the overall 20-30% increase in budget/expenses) triggered by the extended NIS scope, further harmonisation of security requirements and enhanced supervisory activities.</li> <li>• 1-2 FTEs (legal and technical background)</li> </ul>	Regular personnel costs
	Indirect costs	Potential slight increase in prices of products as a result of investment in cybersecurity technologies and measures	n/a	n/a	n/a	n/a	n/a
<b>Action (e)</b> <i>Streamlining incident notifications</i>	Direct costs	n/a	n/a	Personnel costs – potentially 1-2 FTE/organisation	Regular personnel costs	Personnel costs (1-2 FTEs) and potential purchase of software (including for reporting summary of incident reports to ENISA)	Regular personnel costs)

	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (f)</b> <i>Reinforcing and further harmonising supervision and enforcement</i>	Direct costs			Personnel (2FTE/organisation) and purchase costs (in particular for DSPs and SMEs)	Regular personnel costs and potential increase in outsourcing, notably for audits (in particular for SMEs and DSPs) – overall additional 5% of recurrent purchase costs	Part of the overall 20-30% increase in budget/expenses) + administrative costs for the sector-specific decentralised models for the new sectors/services to be added to the NIS scope + 1-2 additional FTEs per competent authority	Personnel Purchase costs Administrative costs
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (g)</b> <i>Incentivising the increase in Member States resources for and prioritising of cybersecurity policies (e.g. peer review and mutual assistance</i>	Direct costs	n/a	n/a	n/a	n/a	<ul style="list-style-type: none"> <li>For the mutual assistance mechanism: 2-3 FTEs per CSIRT team)</li> <li>For the peer-review:</li> </ul>	Personnel and costs triggered by operational activities – in average 5,000 EUR per year per authority for peer-review missions – partially supported

<i>mechanism)</i>							by the EU's Digital Europe Programme
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (h)</b> <i>Strengthening cooperation and information sharing (including through ISACs with public authorities participation)</i>	Direct costs			Personnel costs – 1 extra FTE/organisation	More involvement in the public-private partnerships and ISACs – recurrent personnel costs ( <i>medium level</i> )	Personnel costs – 1-2 FTEs	Regular personnel costs
	Indirect costs						
<b>Action (i)</b> <i>Incentivising coordinated vulnerability disclosure</i>	Direct costs			Negligible personnel costs (could, use existing FTEs who would monitor an additional input channel)	Negligible personnel costs	<ul style="list-style-type: none"> <li>Part of the overall 20-30% increase in budget/expenses) triggered by the extended NIS scope, further harmonisation of security requirements and enhanced supervisory activities.</li> <li>Personnel (1/2 FTEs)</li> <li>Administrative costs</li> </ul>	Regular personnel and purchase/maintenance costs

						• In-house R&D	
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a
<b>Action (j)</b> <i>Setting up a crisis management framework focused on operational cooperation</i>	Direct costs	n/a	n/a	n/a	n/a	Personnel: 3-4 FTEs/national authority and administrative costs	<ul style="list-style-type: none"> <li>• Personnel</li> <li>• Administrative costs (participation in exercises, operational exchange)</li> </ul>
	Indirect costs	n/a	n/a	n/a	n/a	n/a	n/a

(1) Estimates to be provided with respect to the baseline; (2) costs are provided for each identifiable action/obligation of the preferred option otherwise for all retained options when no preferred option is specified; (3) If relevant and available, please present information on costs according to the standard typology of costs (compliance costs, regulatory charges, hassle costs, administrative costs, enforcement costs, indirect costs; see section 6 of the attached guidance).

#### **ANNEX 4: METHODOLOGY AND CRITERIA FOR DETERMINING THE ADDITIONAL SECTORS, SUBSECTORS AND SERVICES CONSIDERED FOR THE NIS SCOPE IN POLICY OPTIONS 2 AND 3**

The additional sectors, subsectors and services were chosen based on:

- (i). the Member States' policy choices to go beyond the scope of the NIS Directive at national level.

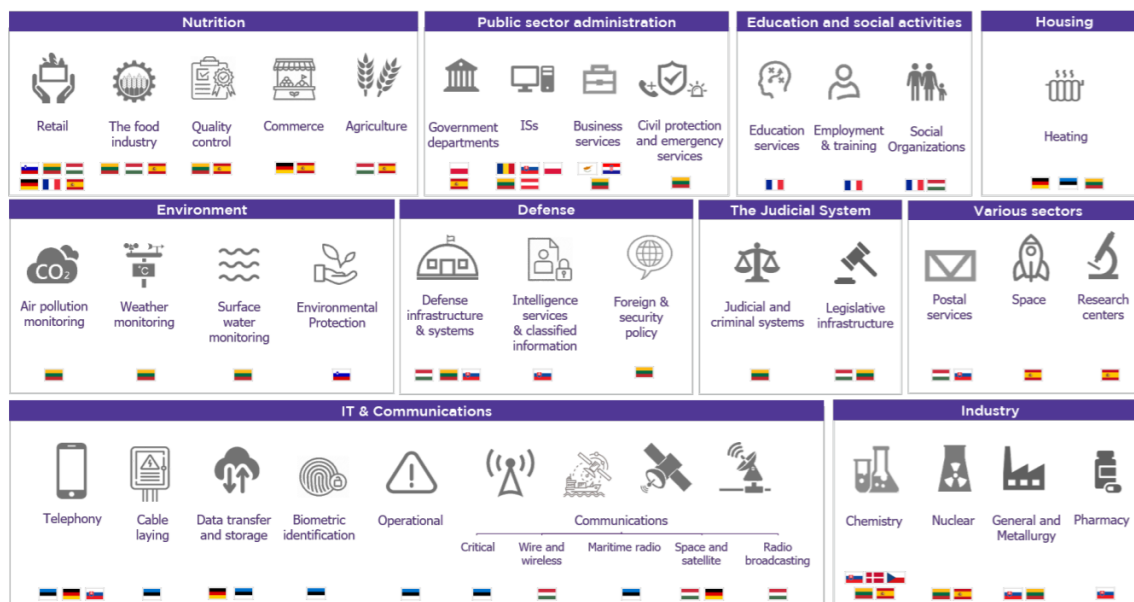
The Commission's Report on OES identification<sup>121</sup> revealed that, at the time of the report, 11 out of 28 Member States have identified essential services in sectors not falling under the scope of Annex II of the NIS Directive. Out of these, 7 have identified a total of 157 OES providing services not covered by the types of entities in Annex II. This is illustrated by the table below.

<b>Additional sector</b>	<b>Examples of entities</b>	<b>Number of Member States</b>
Information infrastructures	Data centres, server farms	5
Financial services (entities not listed in Annex II)	Insurance and reinsurance companies	4
Government services	Electronic services for citizens	4
Heat	Heat producers and suppliers	3
Wastewater	Collection and treatment facilities	3
Logistics	Postal services	2
Food	Producers, trading venues	2
Environment	Disposal of hazardous waste	2
National security/emergency services	112, crisis management	2
Chemical industry	Suppliers and producers of substances	2
Social services	Entities in charge of social benefits	1
Education	Authorities in charge of national exams	1
Collective catering	Distribution management	1
Water	Hydraulic structures	1

In a recent study on the transposition of the NIS Directive, Wavestone (2019)<sup>122</sup> shows that more than half of the Members States have added about 15 subsectors that are not covered by the scope of the NIS Directive.

<sup>121</sup> European Commission (2019), REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems. From now on the "OES Report".

<sup>122</sup> Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665 – implemented by Wavestone, CEPS and ICF.



Source: Wavestone, The NIS Directive, An Overview of Transposition In Europe For Operators Of Essential Services (OESs), June 2020

(ii).stakeholders’ views reflected in the results of the OPC and NIS review study surveys.

The OPC and the NIS review study surveys inquired about the potential addition of sectors in which essential services are being provided.

As regards the sectors and subsectors concerning OES:

➤ The results of the OPC were as follows:

<b><i>Sectors for operators of essential services</i></b>	<b><i>Strongly agree + agree to include the sector in scope of the NIS Directive [%]</i></b>
Public administration	70.8%
Food supply	50.5%
Manufacturing	46.1%
Chemicals	51.5%
Waste water	51.9%
Data centres	68.9%

Furthermore, 50% of the OPC respondents considered that ‘*undertakings providing public communications networks or publicly available electronic communications services currently covered by the security and notification requirements of the EU framework on electronic communication networks and services will be included in the scope of the NIS Directive*’.

- The results of the surveys conducted within the NIS study were as follows:
  - the response from competent authorities is illustrated in the table below



<b><i>Sectors for operators of essential services</i></b>	<b><i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i></b>
Insurance and reinsurance	35%
Chemicals	42%
Manufacturing	32%
Trust services	35%
Food supply	58%
Public Administration	68%
Elections (authorities, technology and process)	48%
Electricity generation	77%
Post and other delivery services	45%
Data centres and Content Delivery Networks (CDN)	65%
Heat production and supply	55%
Wastewater	58%
Waste management	48%
Emergency services	61%
Broadcasting services	52%

- the response from OESs is illustrated in the table below

<b><i>Sectors for operators of essential services</i></b>	<b><i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i></b>
Insurance and reinsurance	42%
Chemicals	50%
Manufacturing	50%
Trust services	58%
Food supply	67%
Public Administration	67%
Elections (authorities, technology and process)	50%

Electricity generation	83%
Post and other delivery services	50%
Data centres and Content Delivery Networks (CDN)	83%
Heat production and supply	50%
Wastewater	67%
Waste management	58%
Emergency services	58%
Broadcasting services	50%

Other sectors and subsectors mentioned by over 10% of the respondents to both OPC and NIS review study surveys:

<b>Other sectors mentioned by the respondents to the OPC and the targeted surveys of the NIS study</b>	<b>%</b>
Wastewater treatment	19% of respondent competent authorities
Energy generation	13% of respondent competent authorities

The results of the surveys conducted within the NIS review study were as follows:

- the response from competent authorities is illustrated in the table below:

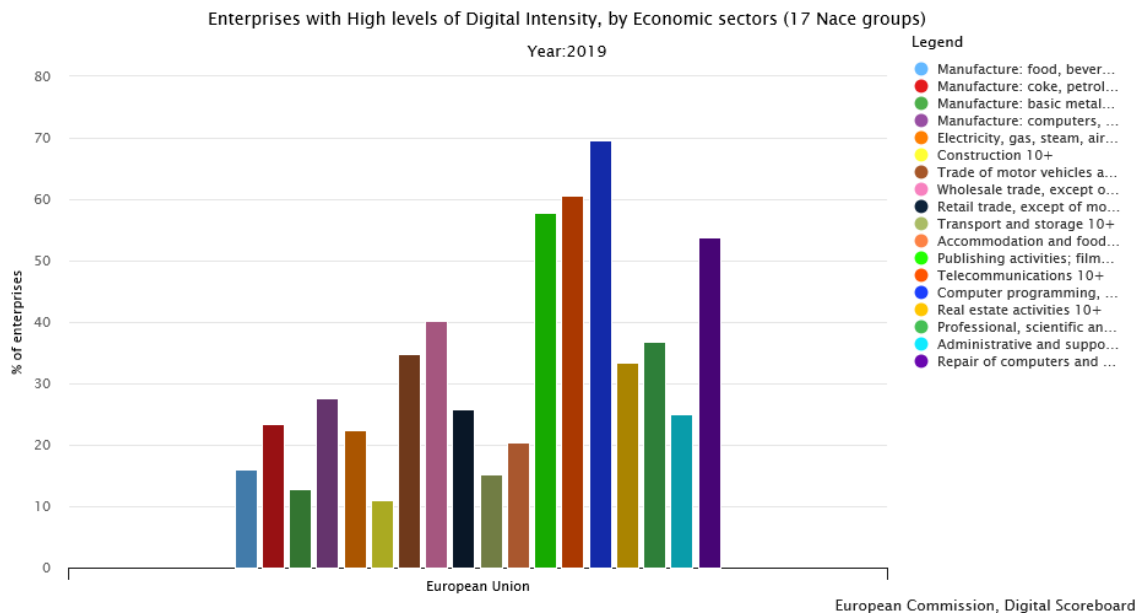
<b>Potential new DSPs</b>	<b><i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i></b>
Geolocation services	86%
Social networks	50%
Data centres and content delivery networks	86%

- the response from DSPs is illustrated in the table below:

<b>Potential new DSPs</b>	<b><i>Agree to some extent, to a moderate extent or to a great extent to include the sector in scope of the NIS Directive [%]</i></b>
Geolocation services	100%
Social networks	100%
Data centres and content delivery	100%

## (iii). sectorial digital intensity

The 2019 data on digital intensity by economic sector of the Digital Economy and Society Index (DESI) was assessed to determine the digital-intensity levels of certain sectors.<sup>123</sup>



Furthermore, the taxonomy of sectors by digital-intensity developed by the OECD in 2018 was also analysed, with the caveats and limitations mentioned further below.<sup>124</sup> See also the following illustrative chart:

<sup>123</sup> [https://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={\"indicator-group\": \"ebusiness\", \"indicator\": \"e\\_di\\_hivhi\", \"breakdown-group\": \"econsector\", \"unit-measure\": \"pc\\_ent\", \"time-period\": \"2019\", \"ref-area\": \[\"EU\"\]}](https://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-breakdowns#chart={\)

<sup>124</sup> OECD, (2018), A taxonomy of digital intensive sectors”, OECD Science, Technology and Industry Working Papers, No. 2018/14, OECD Publishing, Paris, <https://doi.org/10.1787/f404736a-en>. This taxonomy was built using data from 2001-2015 for 36 sectors in 12 OECD countries to create ad hoc indicators. The sectors are classified according to ISIC Rev 4 and the indicators considered were: ICT equipment and software investment relative to fixed investment; intensity in purchase of ICT intermediate goods and services relative to output; stock of robots per employee; number of ICT specialists over total employment and propensity to engage in e-commerce sales.

Taxonomy of sectors by digital-intensity, overall ranking, 2013-15

ISIC Rev.4 industry denomination	Quartile intensity	ISIC Rev.4 industry denomination	Quartile intensity
Agriculture, forestry, fishing	Low	Wholesale and retail trade, repair	Medium-high
Mining and quarrying	Low	Transportation and storage	Low
Food products, beverages and tobacco	Low	Accommodation and food service activities	Low
Textiles, wearing apparel, leather	Medium-low	Publishing, audiovisual and broadcasting	Medium-high
Wood and paper products, and printing	Medium-high	Telecommunications	High
Coke and refined petroleum products	Medium-low	IT and other information services	High
Chemicals and chemical products	Medium-low	Finance and insurance	High
Pharmaceutical products	Medium-low	Real estate	Low
Rubber and plastics products	Medium-low	Legal and accounting activities, etc.	High
Basic metals and fabricated metal products	Medium-low	Scientific research and development	High
Computer, electronic, optical products	Medium-high	Advertising and other business services	High
Electrical equipment	Medium-high	Administrative and support service	High
Machinery and equipment n.e.c.	Medium-high	Public administration and defence	Medium-high
Transport equipment	High	Education	Medium-low
Furniture; other manufacturing; repairs	Medium-high	Human health activities	Medium-low
Electricity, gas, steam and air cond.	Low	Residential care and social work activities	Medium-low
Water supply; sewerage, waste	Low	Arts, entertainment and recreation	Medium-high
Construction	Low	Other service activities	High

Source: Calvino et al. (2018) based on Annual National Accounts, STAN, ICIO, PIAAC, International Federation of Robotics, World Bank, Eurostat Digital Economy and Society Statistics, national Labour Force Surveys, US CPS, INTAN-Invest and other national sources.

However, the above-mentioned index also has its limitations, having been built with data dating back to 2015. Therefore, it does not take into account, for instance, the profound digital transformation of certain sectors due to the increasing use of IoT and AI.















- (iv). level of importance for society of sectors, subsectors and services revealed by major crisis and in particular COVID-19

To complement the above-mentioned factors, consideration was also given to the role the sectors, subsectors and services have played during the COVID-19 crisis. The unprecedented nature and scale of this crisis stressed once more the criticality of sectors such as healthcare, which faced an increasing level of cyber threats, while at the same time revealed the importance for society of other sectors, such as food distribution and supply, in spite of these not showing a high degree of connectivity with other sectors. The analysis of this criterion was therefore mainly a qualitative one, taking account of the national authorities' decisions to qualify certain sectors or types of services as essential for society during the imposition of restrictive measures aimed at reducing the spread of the COVID-19 pandemic.

- (v). interdependency among sectors, notably in regard of digital infrastructures and DSPs

For this criterion, ENISA's assessment of the interdependencies between the OESs and DSPs was considered<sup>125</sup>. The figure below illustrates ENISA's conclusions with regard to dependencies among OES and DSPs.

<sup>125</sup> *Good practices on interdependencies between OES and DSPs*, ENISA, November 2018: <https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps>

OPERATOR OF ESSENTIAL SERVICES			DIGITAL SERVICE PROVIDERS		
Sector	Subsector		Online marketplace 	Online search engine 	Cloud computing service 
 Energy	Electricity 		●	●	●
	Oil 		●	●	●
	Gas 		●	●	●
 Transport	Air Transport 		●	●	●
	Rail Transport 		●	●	●
	Water Transport 		●	●	●
	Road Transport 		●	●	●
Drinking water supply and distribution			●	●	●
Digital infrastructure			●	●	●

● Low ● Medium ● Medium-High

Source: ENISA - Dependencies of Operators of Essential Services on Digital Service Providers (overview)<sup>126</sup>

Based on the above-mentioned criteria, a scoring from 0 to 2 per criterion was attributed to each of the potentially new sectors, subsectors and services, as follows:

- on the Member States’ policy choices to go beyond the scope of the NIS Directive at national level – a score of 0 if no Member State added the sector/subsector/service, 1 if 1 or 2 Member States added that sector, 2 if 3 Member States or more added it.
- on the stakeholders’ views reflected in the results of the OPC and/or in the targeted surveys for competent authorities, OES and DSPs:
  - 0 if less than 35% of the OPC respondents agreed or strongly agreed and/or, in the case of the targeted consultations of the NIS review study, if 35% and fewer of the median of the two relevant categories (i.e. competent authorities and operators of essential services or competent authorities and digital service providers) of responding stakeholders agreed to some extent, a moderate extent or a great extent;
  - 1 if between 35 and 50% of the OPC respondents agreed or strongly agreed and/or, in the case of targeted consultations of the NIS review study, if between 35% and 50% of the median of the three categories (or, as applicable, two categories) of responding stakeholders agreed to some extent, a moderate extent or a great extent;

<sup>126</sup> Figure 4, page 14 of ENISA’s *Good practices on interdependencies between OES and DSPs*, November 2018.

- 2 if over 50% of the OPC respondents agreed or strongly agreed and/or, in the case of targeted consultations of the NIS review study, if over 50% of the median of the three categories (or, as applicable, two categories) of responding stakeholders agreed to some extent, a moderate extent or a great extent.
- on sectorial digital intensity, DESI and the OECD data were cumulatively considered: 0 for low, 1 for medium-low and medium 2 for medium-high and high. For sectors where several subsectors were highlighted in the sources mentioned above, an average score for the overall sector was considered. For sectors and services not covered by the above-mentioned indexes, reasonable assumptions were made.
- on the level of importance for society of sectors, subsectors and services revealed by major crisis and in particular COVID-19: 0 for very little to no importance; 1 for relative importance and 2 for high importance;
- on interdependency among sectors, notably in regard of digital infrastructures and DSPs and exposure to cybersecurity risks: 0 for low to no level of reliance of other sectors/subsectors on the given sector/subsector and impact of potential threats; 1 to relative level and 2 for high level.

The sectors, subsectors and services totalling **5 points or higher out of the total of 10**. These results are marked in the table below.

Geolocation services, while they scored sufficiently high to be considered for the NIS scope, notably due to the high scores in the consultations and surveys, were eventually not considered for any of the policy options. This is because it was not possible to define with sufficient precision the type of providers or sectors these would belong to.

In addition to the sectors, subsectors and services subject to the NIS review consultations mentioned above and reflected in the scoring table below, operators of government-owned and privately-owned **ground-based infrastructure that support the provision of space-based services** were also considered to be added to the NIS scope, also in consideration of the consistency with the review of the Directive on the identification and designation of European critical infrastructures.<sup>127</sup> Ground-based infrastructure performs essential functions, including control, monitoring, tracking and data collection activities. Space-based services are playing an increasingly important role for the economy and society as a whole and are important for the daily operations of many other critical and important entities. The sector exhibits a very high degree of digital intensity and its operators are highly interconnected with other parts of the economy, making them a likely target for cyber-attacks. Given the large economies of scale that prevail in the provision of space-based services, the sector also exhibits a particularly strong pan-European dimension.

Furthermore additional **subsectors** would also be added for the energy sector, and in particular: district heating, electricity generation, central oil stockholding entities, nominated electricity market operators and electricity market participants providing aggregation, demand response or energy storage services, operators of hydrogen production storage and transmission, as well as EU reference laboratories and entities

---

<sup>127</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82.

conducting research and development activities of medicinal products for the healthcare sector.

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

<i>Sector/subsector/service</i>	Added by Member States	Consultation results (OPC and/or targeted surveys)	Digital intensity	COVID-19 crisis related importance	Level of interdependency of other sectors/subsectors	<b>TOTAL</b>
Electronic communication networks and services <sup>128</sup> (including emergency communication)	2	2	2	2	2	<b>10</b>
Insurance and reinsurance (as part of financial services)	2	n/a	1	0	0	3
Chemicals	2	2	1	0	0	<b>5</b>
Manufacturing	2	1	1	1	1	<b>6</b>
Food supply	2	2	1	2	0	<b>7</b>
Public Administration <sup>129</sup>	2	2	1	1	1	<b>7</b>
Electricity generation	1	2	1	2	1	<b>7</b>
Education (e.g. certain authorities such as those in charge of national exams)	1	n/a	1	0	0	2
Post and other delivery services	1	1	1	2	1	<b>6</b>

<sup>128</sup> This also includes broadcasting services.

<sup>129</sup> This also includes elections (authorities, technology and process), as covered by the consultations, and to the extent they are part of public administration as defined at national and/or regional levels.



Heat production and supply	2	2	1	1	1	<b>7</b>
Wastewater	2	2	0	1	0	<b>5</b>
Waste management	1	2	0	1	1	<b>5</b>
Emergency services	1	2	1	2	0	<b>6</b>
Online media	0	n/a	2	2	0	4
Data centres & Content Delivery Networks	2	2	2	2	2	<b>10</b>
Geolocation services	0	2	2	0	1	<b>5</b>
Social networks	0	2	2	1	0	<b>5</b>
Trust service providers	0	1	2	0	2	<b>5</b>

## ANNEX 5: EVALUATION REPORT

# EVALUATION OF DIRECTIVE (EU) 2016/1148 CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION ("NIS DIRECTIVE ")

### Table of contents

a)	Introduction .....	84
	Purpose and scope .....	84
b)	Background to the intervention .....	85
	Description of the intervention and its backgrounds .....	85
	The adoption and implementation context .....	86
	Intervention logic of the NIS Directive .....	90
	Baseline and points of comparison.....	91
c)	Implementation / state of Play .....	92
	Description of the current situation .....	92
d)	Method.....	105
	Short description of methodology .....	105
	Deviations from the Roadmap.....	106
	Limitations and robustness of findings .....	107
e)	Analysis and answers to the evaluation questions.....	107
	Relevance .....	107
	Coherence .....	110
	EU Added Value .....	111
	Effectiveness .....	113
	Efficiency .....	115
f)	Conclusions .....	116

## Glossary

<i>Term or acronym</i>	<i>Meaning or definition</i>
CDN	Content delivery network
CSIRTs	Computer Security Incident Response Teams
DNS	Domain Name System
DORA	Digital Operational Resilience Act for the financial sector
DSP	Digital service provider
The ECI Directive	The Directive on the identification and designation of European critical infrastructures
EASA	The European Union Aviation Safety Agency
EECC	European Electronic Communications Code
eIDAS (Regulation)	Regulation on electronic identification and trust services for electronic transactions in the internal market
ENISA	The European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
ICT	Information Communication Technology
ISAC	Information Sharing and Analysis Centre
ISO	International Organisation for Standardisation
IXP	Internet Exchange Points
MeliCERTes	Cybersecurity Digital Service Infrastructure Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs
NCA	National Competent Authority
NIS Directive	Directive concerning measures for a high common level of security of network and information systems across the Union
OES	Operator of essential services

PPP	Public Private Partnerships
PSD2	Payment Services Directive 2
SME	Small and medium-sized enterprises
SPOC	Single Point of Contact
TFEU	Treaty on the Functioning of the European Union
TLD	Top-level domain

## a) INTRODUCTION

### **Purpose and scope**

Directive (EU) 2016/1148<sup>130</sup> concerning measures for a high common level of security of network and information systems across the Union (“NIS Directive” or “the Directive”) is the first horizontal internal market instrument aimed at improving the cybersecurity resilience of the European Union. Adopted in July 2016, the NIS Directive has ensured the continuity of essential services allowing the European Union's economy and society to function properly, building cybersecurity capabilities across the EU and mitigating growing threats to network and information systems used to provide essential services in key sectors.

Article 23 of the Directive requires the European Commission to review the functioning of the Directive periodically and to report to the European Parliament and the Council for the first time by 9 May 2021. Meanwhile, the speedy digital transformation of our society has expanded the threat landscape and is bringing about new challenges, which require adapted and innovative responses. The COVID 19 crisis and the resulting sudden growth in demand for internet-based solutions has emphasised even more the need for a state of the art cybersecurity. Therefore, as part of its key policy objective to make “Europe fit for the digital age”, the Commission announced in its Work Programme 2020 that it would advance the review of the Directive to the end of 2020<sup>131</sup>.

The evaluation process started already mid 2019 with the Commission’s “NIS country visits” across all Member States and with a Report from October 2019 assessing the consistency of the approaches in the identification of operators of essential services<sup>132</sup> (“the OES Report”), which was adopted pursuant to Article 23(1) of the Directive. The implementation of the NIS Directive has been the subject of the discussions with the Member States’ competent authorities and ENISA in the NIS Cooperation Group. The present Evaluation Report also takes into account the reports from the Cooperation Group and CSIRTs Network on the experience gained at a strategic and operational level.<sup>133</sup>

The Commission carried out an open public consultation collecting views from all stakeholders. A wide range of stakeholders were consulted as part of the evaluation. These included competent authorities from the Member States, operators from all sectors

---

<sup>130</sup> Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJL 194/1, 19.7.2016.

<sup>131</sup> COM (EU) (2020) 37 final, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Commission Work Programme 2020, Brussels, 29.1.2020.

<sup>132</sup> COM (EU) 2019/546 final, Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, Brussels, 28.10.2019.

<sup>133</sup> See Article 23 (2) NIS Directive. According to Articles 11 (4) and 12 (4), the Cooperation Group and the CSIRTs Network have to report on the experiences gained respectively with the strategic and operational cooperation by 9 August 2018 and every year and a half thereafter. Both the Cooperation Group as well as the CSIRTs Network have reported twice on their respective experiences gained (in August 2018 and in January 2020).

under the Directive and Member States, digital service providers, academia and think tanks and the general public. The Commission was supported by an external study<sup>134</sup>, which carried out targeted surveys and interviews and organized dedicated workshops and finally provided input to the evaluation and drafting of the impact assessment.

The review evaluates the functioning of the NIS Directive based on the level of security of network and information systems in the Member States. In accordance with the Better Regulation Guidelines, the evaluation assesses the effectiveness, efficiency, coherence, relevance and EU added value of the NIS Directive taking into account the constantly evolving technological and threat landscape. It pays attention to the impact of the NIS Directive on increasing the levels of cybersecurity across the Union, in particular on the level of national cybersecurity capabilities and the capacity to mitigate growing security threats to network and information systems used to provide essential services in key sectors. The evaluation elaborates on the lessons learned from the implementation of the NIS Directive and identifies persisting and emerging issues affecting the functioning of the Directive. The evaluation also attempts to identify and quantify the direct and indirect regulatory costs and benefits resulting from the implementation of the NIS Directive.

The evaluation focuses on the period starting from the end of the transposition deadline in May 2018 and covers all Member States. Depending on the results from the evaluation of the functioning of the NIS Directive and an impact assessment, the Commission might propose measures aimed at enhancing the level of cybersecurity within the Union.

This staff working document describes the evaluation, how it was carried out, and what it found.

## **b) BACKGROUND TO THE INTERVENTION**

### **Description of the intervention and its backgrounds**

Based on Article 114 of the Treaty on the Functioning of the European Union (TFEU)<sup>135</sup>, the NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU, in order to contribute to the overall functioning of the internal market, by ensuring:

- a) a high level of preparedness of Member States by requiring them to adopt a national strategy on the security of network and information systems and designate: one or more national Computer Security Incident Response Teams (CSIRTs) responsible for risk and incident handling, a single point of contact (SPOC) which shall exercise a liaison function to ensure cross-border cooperation between the Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group, and a competent national NIS authority;
- b) cooperation among all the Member States by establishing the Cooperation Group to support and facilitate strategic cooperation and the exchange of information among

---

<sup>134</sup> An external study carried out by a consortium of Wavestone, ICF and the Centre for European Policy Studies (CEPS), supported the Commission during the evaluation and impact assessment process. The study kicked off in April 2020 and should be finalised by January 2021. The final report of the study was not yet submitted at the time of writing of this report.

<sup>135</sup> Treaty on the Functioning of the European Union, OJ C 326/47, 26.10.2012.

- Member States, and the CSIRTs Network, which promotes swift and effective operational cooperation between national CSIRTs; and
- c) a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure.

Public and private entities identified by the Member States as operators of essential services (OESs) in these sectors are required to undertake a risk assessment and put in place appropriate and proportionate security measures as well as to notify serious incidents to the relevant authorities. Also providers of key digital services (DSPs) such as search engines, cloud computing services and online marketplaces have to comply with the security and notification requirements under the Directive; at the same time, the latter are subject to a so-called ‘light-touch’ regulatory regime which entails, among others, that they are under the jurisdiction of one Member State for the whole EU and are not subjected to ex-ante supervisory measures.

### **The adoption and implementation context**

Cybersecurity resilience is a key priority for the protection of critical infrastructure in the European Union, where network and information systems could be vulnerable due to the fragmented nature of national strategies and capabilities. At a time when the private and public sectors rely increasingly on digital infrastructure for the delivery of essential services, those become major targets of cyberattacks. The companies’ incentives to invest in cybersecurity are insufficient and the benefits of the disclosure of incidents and data breaches – more efficacy and cost savings in security – usually are slower and benefit all firms (including competitors). Ultimately, in an interconnected society, only a collective and coordinated effort between private and public organisations, and national and European players can lead to sufficient levels of cybersecurity resilience.

Against this background, the EU started building the foundations of its current cybersecurity policy. In 2004, the European Network and Information Security Agency (ENISA), was founded. In 2009, the Commission’s Communication was adopted, which focuses on awareness and defines an immediate action plan to strengthen the European cybersecurity resilience<sup>136</sup>. This Communication was followed in 2013 by the joint Communication on a Cybersecurity Strategy to guide the Union’s policy response to cyber threats and risks<sup>137</sup>.

As part of this package, the Commission adopted a Proposal for Directive concerning measures to ensure a high common level of network and information security across the Union<sup>138</sup>. After almost three years of negotiations, a political agreement was reached at the end of 2015, with the understanding that approach to cybersecurity limited to the

---

<sup>136</sup> COM (EU) (2009) 149 final, Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection “Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Brussels, 30.3.2009.

<sup>137</sup> JOIN (EU) (2013) 1 final, Joint Communication to the European Parliament, the Council the European Economic and Social Committee and the Committee of the regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013.

<sup>138</sup> COM (2013) 48 final, SWD (2013) 31 final of 7 February 2013.

national dimension could have put the Digital Single Market at risk<sup>139</sup>. The finally adopted NIS Directive was ground-breaking as it was the first EU legislative act to regulative cybersecurity across sectors. It also complemented the protection of personal data, privacy, the provision of electronic communications services and electronic interactions between businesses, citizens and public authorities offered respectively by the General Data Protection Regulation (GDPR)<sup>140</sup>, the E-Privacy Directive<sup>141</sup>, the Framework Directive on electronic communications networks and services<sup>142</sup> and the eIDAS Regulation<sup>143</sup>.

The NIS Directive has laid the foundations for a European cybersecurity framework and emphasised the need for Member States to secure their own infrastructures in order to function consistently across the European Union. At the same time, the Directive has left large room for discretion to Member States in the implementation of the Directive's objective by requiring a minimum level of harmonisation of the actions to be put in place (Article 3).<sup>144</sup>

To reduce the degree of divergence in the implementation between European countries, a Cooperation Group made up of national representatives, ENISA<sup>145</sup>, and the European Commission, has been tasked to provide strategic direction<sup>146</sup> including guidance on transposition of the Directive (Article 11); and a network of CSIRTs have also been created to ensure that good practice is communicated and exchanged, as well as to support Member States in the implementation of the Directive (Article 12)<sup>147</sup>.

---

<sup>139</sup> Sumroy, R., Donovan, N., (2015), "The NIS Directive: Genesis, Status and Key Aspects", *Slaughter & May*, Briefing June 2015.

<sup>140</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJL 119/1, 4.5.2016.

<sup>141</sup> Directive (EU) 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJL 201/37, 31.7.2002.

<sup>142</sup> DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJL 108, 24.4.2002, p. 33–50.

<sup>143</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG)

<sup>144</sup> With the exception of security or notification requirements on digital service providers, regarding which the Member States shall not impose any further requirements than those prescribed by the NIS Directive, see Article 3 and Article 16(10) of the NIS Directive.

<sup>145</sup> ENISA has become the European Union Agency for Cybersecurity, with a new permanent mandate, and it has been able to perform new tasks as defined by the EU Cybersecurity Act, which entered into force in June 2019.

<sup>146</sup> See Article 11 of the NIS Directive; Commission Implementing Decision (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

<sup>147</sup> Billois, G., (2017), "Cybersecurity and the NIS Directive. A challenge of Consistency for the European Union", Letter from the Wavestone Cybersecurity and Digital Trust Consultant. *Risk Insight*. at: <https://uk.wavestone.com/app/uploads/2017/02/cybersecurity-nis-directive-europe-2.pdf> (last accessed on 21.05.2020).



By establishing a background for cooperation and helping Member States with lower cybersecurity maturity levels to develop their cybersecurity capabilities, the NIS Directive has triggered mind-set change in relation to cybersecurity. Even if cybersecurity, national security and state-sovereignty are still perceived as closely related, the NIS Directive has managed to overcome past concerns regarding sovereign control, helping Member States to experience the benefits of acting together at EU level.

Furthermore, since the adoption of the Cybersecurity Strategy and the last extension of ENISA's mandate in 2013, the overall policy context has changed significantly as the global environment has become more uncertain and less secure. In view of the growing role of ENISA as a reference point for advice and expertise, as a facilitator of cooperation and of capacity-building as well as within the framework of the new Union cybersecurity policy, it became necessary to review ENISA's mandate, to establish its role in the changed cybersecurity ecosystem and to ensure that it contributes effectively to the Union's response to cybersecurity challenges emanating from the radically transformed cyber threat landscape.<sup>148</sup> As a result, the Cybersecurity Act<sup>149</sup> adopted in 2019 granted a permanent mandate to ENISA, more resources and new tasks. The Cybersecurity Act also introduced for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes.

In July 2020, the Commission adopted the EU Security Union Strategy<sup>150</sup>, which acknowledged the increasing interconnection and interdependency between physical and digital infrastructures, and underlined the need for a more coherent approach between specifically the NIS Directive and the European Critical Infrastructure Directive (ECI Directive). The 2019 evaluation of the ECI Directive<sup>151</sup> showed that the landscape related to critical infrastructure protection has changed since the adoption in 2008. To this end, the Commission Work Programme 2020<sup>152</sup> has also planned a proposal for additional measures on critical infrastructure protection until the end of 2020<sup>153</sup>.

The EU Security Union Strategy also underlines the importance of sector-specific initiatives to tackle the specific risks faced by critical infrastructures and to accompany the horizontal frameworks. One such initiative is the Proposal for a Regulation on Digital

---

<sup>148</sup> See Recital 16 of REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

<sup>149</sup> REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

<sup>150</sup> Communication on the EU Security Union Strategy, COM(2020) 605, 24 July 2020 (Strategic priority 'A future-proof security environment').

<sup>151</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. The objective of the Directive is to strengthen the protection of critical infrastructures in the energy and transport sectors.

<sup>152</sup> COM (EU) (2020) 37 final, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Commission Work Programme 2020, Brussels, 29.1.2020.

<sup>153</sup> Security Union Strategy of 24 July 2020, <https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf>; DG HOME, Roadmap regarding new rules regarding the protection of critical infrastructure in the EU, <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12462-Enhancement-of-European-policy-on-critical-infrastructure-protection>

Operational Resilience for the financial sector (DORA)<sup>154</sup>, which is part of the digital finance package<sup>155</sup>, adopted on 24 September 2020. DORA aims at strengthening the digital operational resilience of the EU financial sector entities, including their ICT security, by streamlining and upgrading existing rules and introducing requirements where gaps exist. DORA would constitute a *lex specialis* to the NIS Directive, at the same time ensuring that details of significant incidents would be passed on from the competent financial authorities to the SPOCs under the NIS Directive and that there will be exchange of information between the financial authorities and the NIS authorities within the framework of the NIS Cooperation Group. In addition, as part of the digital finance package, the Commission put forward a digital finance strategy and a legislative proposal on Crypto Assets aiming to increase the robustness of digital services against cyberattacks<sup>156</sup>.

Other sectorial initiatives are the Network code for the cybersecurity of cross-border electricity flows<sup>157</sup> and the initiative on the protection and cybersecurity of critical energy infrastructure.

Furthermore, in the transport sector, the Union adopted detailed rules for cybersecurity in the aviation security domain<sup>158</sup>. The EU Aviation Safety Agency (EASA) is preparing an opinion to be submitted to the European Commission in order to amend aviation safety legislation with cybersecurity provisions requiring the mandatory introduction of an Information Security Management System.

Last but not least, the Framework Directive<sup>159</sup>, which was amended by the European Electronic Communication Code<sup>160</sup>, also requires Member States to ensure that operators falling under its scope take the necessary risk management measures to secure their networks and to report significant incidents. However, the NIS Directive obligations do not apply as far as the provision of public electronic communication networks or of publicly available electronic communication services are concerned (Article 1 (3) NIS Directive).

---

<sup>154</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 of 24 September 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1>

<sup>155</sup> [https://ec.europa.eu/info/publications/200924-digital-finance-proposals\\_en](https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en)

<sup>156</sup> Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. [https://ec.europa.eu/finance/docs/law/200924-crypto-assets-proposal\\_en.pdf](https://ec.europa.eu/finance/docs/law/200924-crypto-assets-proposal_en.pdf)

<sup>157</sup> As empowered by Regulation (EU) 2019/943 on the internal market for electricity. Preparatory work was finalised in September 2019, an informal drafting process is ongoing.

<sup>158</sup> Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2019.246.01.0015.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.246.01.0015.01.ENG)

<sup>159</sup> DIRECTIVE 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended in 2009, OJ L 108, 24.4.2002, p. 33–50.

<sup>160</sup> See Article 40 of DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code.

## Intervention logic of the NIS Directive

The intervention logic presented in the below chart aims to depict the chain of expected effects associated with the NIS Directive.<sup>161</sup>

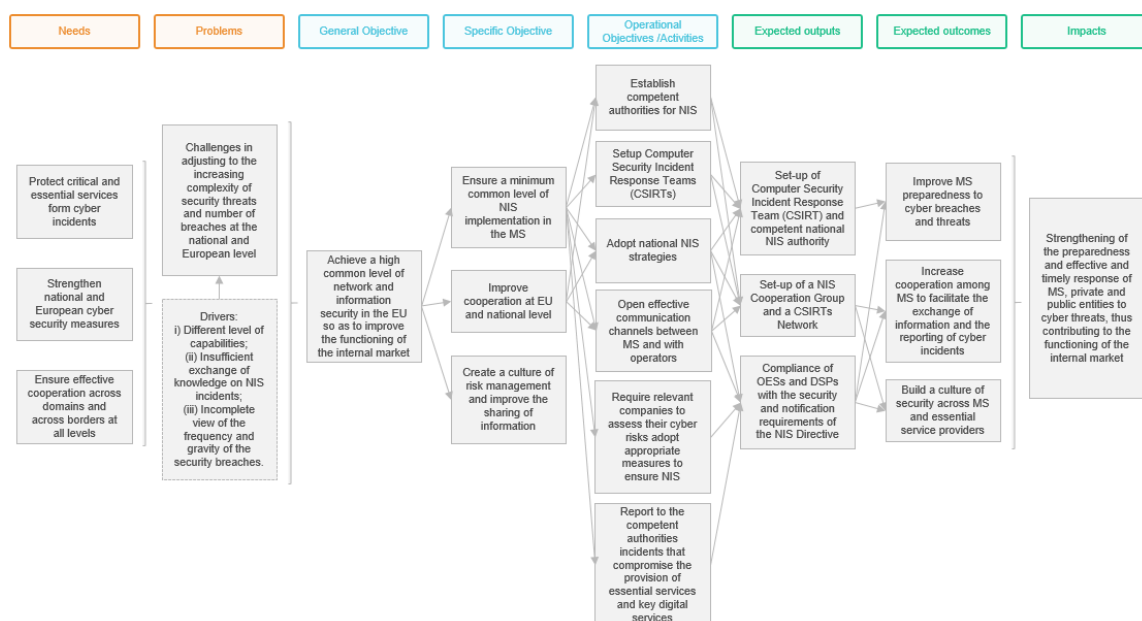


Figure 1: The NIS Directive intervention logic

The above chart helps in visualising the *problem* that the Directive was intended to address when it was first adopted, namely the overall insufficient level of protection against network and information security incidents, risks and threats across the EU undermining the proper functioning of the Internal Market.

It looks at the *drivers* behind the problems: the significant disparities in Member States' capabilities and level of preparedness, the insufficient sharing of information on cybersecurity incidents and threats between Member States and key operators and digital service providers and the incomplete view of the frequency and gravity of the security incidents.

Most importantly, it flags the *main objectives* of the Directive. The general objective of guaranteeing a high common level of security on network and information systems in the Union could be translated into *specific objectives* and further *operational objectives*. The specific objectives are (1) to ensure a minimum common level of security of network and information systems implementation in the Member States and thus increase the overall level of preparedness and response, (2) to improve cooperation at Union and at national level with a view to counter cross-border incidents and threats effectively and (3) to create a culture of risk management and sharing of information by OES and DSPs. They should be achieved via the establishment of national competent authorities, CSIRTs, the adoption of national strategies, the creation of links and communication channels

<sup>161</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

between the Member States and with the operators (e.g. via the process of identification), establishing risk management and incident reporting requirements on operators.

These objective should have translated into specific *outputs* leading to *outcomes*, such as improving Member States preparedness to cyber incidents, increased cooperation and information exchange and building a culture of security across Member States and among essential operators and digital service providers. The overall *impact* of the NIS Directive is to strengthen the preparedness of EU Member States and companies and ensure an effective and timely response to cyber threats, thus contributing to the functioning of the Internal Market.

### **Baseline and points of comparison**

The increasing importance of the security of network and information systems for our economies and societies was recognised for the first time by the Commission in 2001, with the Communication ‘Network and Information Security: Proposal for A European Policy Approach’<sup>162</sup> that stressed the increasing importance of network and information systems’ security for our economies and societies. Furthermore, the EU became an observer to the Council of Europe’s Convention on Cybercrime Committee in 2001, and since 2002, legislation related to cybersecurity matters has been adopted<sup>163</sup>. Before the starting of the process that lead to the adoption of the NIS Directive<sup>164</sup>, the only sector where companies were required to take cybersecurity risk management steps under EU law was the electronic communications sector, regulated at the time by the Framework Directive 2002/21/EC on electronic communications networks and services<sup>165</sup> but there was no horizontal instrument aimed at improving the cybersecurity resilience of the Union.

In order to ensure a high and effective level of network and information security in the EU, the European Network and Information Security Agency (ENISA)<sup>166</sup> was established in 2004. The approach adopted at that stage by the European Union in the area of network and information systems has mainly consisted in the adoption of a series of action plans and strategies urging the Member States to increase their cybersecurity capabilities and to cooperate to counter cross-border cybersecurity problems.<sup>167</sup>

---

<sup>162</sup> COM (EU) 2001/0298 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach, Brussels, 6.6.2001.

<sup>163</sup> European Court of Auditors (2019), Challenges to Effective EU Cybersecurity Policy, Briefing Paper, No 02/2019. Available at [https://www.eca.europa.eu/Lists/ECADocuments/BRP\\_CYBERSECURITY/BRP\\_CYBERSECURITY\\_EN.pdf](https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf) (last accessed on 17.06.2020).

<sup>164</sup> COM (EU) (2009) 149 final, Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection ‘Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, Brussels, 30.3.2009.

<sup>165</sup> Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJL 108/33, 24.4.2002.

<sup>166</sup> The Cybersecurity Act changed ENISA’s name to the European Union Agency for Cybersecurity.

<sup>167</sup> COM (EU) (2013) 48 final, Proposal for a Directive Of The European Parliament And Of The Council concerning measures to ensure a high common level of network and information security across the Union, Brussels, 7.2.2013.

In 2015, before the NIS Directive was adopted, almost one third of the Member States did not have a cybersecurity national strategy. Only a small group of Member States had adopted legislation and policy initiatives to address security of networks and information systems.<sup>168</sup> Many Member States did not have an operational CSIRT to deal with cybersecurity incidents. In 2015, there were no common security and notification requirements on OES and DSPs with the exception of telecommunications companies. In 2015, the majority of the Member States have not done a risk analysis of their assets to determine which national infrastructures were considered to be critical for the functioning of the economy and society<sup>169</sup>.

Without the adoption of the NIS Directive, i.e. under a voluntary approach, the Commission, with the support of ENISA, could have made use of soft law measures such as for example recommendations or guidelines to encourage the Member States to reach a minimum harmonisation of cybersecurity, to set up CSIRTs, and to adopt a national cyber security strategy.

However, doing so, it would have been unlikely that all the Member States would have improved their national capabilities and preparedness. Cross-border cooperation efforts and coordination across all EU Member States to respond to risks and incidents would have taken place only to a very limited extent. It is also less probable that key private players would have managed security risks as effectively as they have done after the introduction of requirements to implement cybersecurity risk management.

Given the interdependency of European networks and systems, with a voluntary cooperation and a voluntary alignment of cybersecurity requirements, the negative impact of cybersecurity incidents and threats on the EU economy and society could have been significant, with the risk of undermining trust in the digital agenda and endangering the Internal Market.<sup>170</sup>

## **c) IMPLEMENTATION / STATE OF PLAY**

### **Description of the current situation**

#### **Implementation process**

The NIS Directive was adopted in July 2016 and entered into force in August 2016. Member States had until 9 May 2018 to adopt national measures necessary to comply with provisions of the Directive. 17 Member States had not communicated transposition by this deadline. The Commission started infringement procedures by sending letters of formal notice to these Member States in July 2018. By September 2019, all Member States had communicated full transposition.

---

<sup>168</sup> BSA, the Software Alliance (2015), EU Cyber security Dashboard: A Path to a Secure European Cyberspace. Available at: [http://cybersecurity.bsa.org/assets/PDFs/study\\_eucybersecurity\\_en.pdf](http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf).

<sup>169</sup> COM (EU) 2019/546 final, Report From The Commission To The European Parliament And The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, Brussels, 28.10.2019.

<sup>170</sup> SWD (EU) 2013/032 final, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, Strasbourg, 7.2.2013.

In the context of the implementation of the NIS Directive, Member States were required to define essential services and identify operators of essential services in their territories based on criteria set up in the Directive. Article 5(7) of the Directive requires Member States to report to the Commission on the results of this identification. In accordance with Article 23(1), the Commission was tasked to draft a report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services (“the OES Report”) and to submit it to the European Parliament and the Council by 9 May 2019. The OES Report was based on an assessment conducted between November 2018 and September 2019. In view of these delays in the identification process and the lacking information from a number of Member States, the report was only published on 28 October 2019.

In July 2019, the Commission sent letters of formal notice to 6 Member States for failure to comply with their obligations under Article 5(7). At the time of drafting of the present Evaluation Report, 3 of the started infringement procedures are still ongoing.

In addition to the OES Report, in view of its obligation under Article 23(2) to report on the functioning of the Directive, the Commission has been carrying out “NIS country visits” across the Member States from June 2019 to July 2020<sup>171</sup>. During these country visits aiming to assess on the spot the level of transposition and implementation of the NIS Directive and to receive feedback both from the industry and the relevant authorities about the effects and challenges brought by the Directive, the Commission interviewed various stakeholders – OES from different sectors, DSPs, national competent authorities, SPOCs and CSIRTs.

### **Implementing and transposing measures**

*National capabilities – national strategies, setting up of national competent authorities, SPOC and CSIRT*

The NIS Directive requires Member States to adopt a *national cybersecurity strategy* containing at least<sup>172</sup> the seven elements listed in Article 7(1) and to communicate this to the Commission. In 2015, only 19 out of the then 28 Member States had national strategies in place, 8 Member States did not have any strategy and one Member State was in the process of drafting a national strategy<sup>173</sup>. With the implementation of the Directive, all Member States have developed specific national legislation to regulate several aspects of cybersecurity and to put in place concrete initiatives in this direction by assigning the role to each body. Therefore, the adoption of the national strategies gave impetus to the implementation of a series of concrete policy actions such as the definition of a risk-assessment plan, a governance framework to achieve the objectives of the national strategy and the identification of measure related to cybersecurity capacity building such as preparedness, response and recovery<sup>174</sup>. This legal provision helped the Member States

---

<sup>171</sup> Due to the COVID-19 crisis, 12 out of the 27 NIS country visits were carried out in a virtual format.

<sup>172</sup> Communication from the Commission to the European Parliament and the Council, “Making the most of NIS”, COM (2017) 476 final 24 October 2017, p. 6.

<sup>173</sup> Business Software Alliance (2015), EU Cyber security Dashboard: A Path to a Secure European Cyberspace.

<sup>174</sup> Bird & Bird (2020), Developments on NIS Directive in EU Member States and ENISA- (2020) National Cyber Security Strategies- Interactive Map. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

with less capacity to make a substantial step forward in cybersecurity preparedness, ensuring a high level of security in their territory.<sup>175</sup>

The NIS Directive also requires Member States to designate one or more *competent authorities* to implement the provisions of the Directive for the key sectors and digital services under its scope. In addition, Member States have to put in place a single point of contact (SPOC) for cross-border cooperation and one or more *computer security incident response teams (CSIRTs)* for incident handling.

All Member State now have designated NCAs, a SPOC and CSIRT(s)<sup>176</sup>. However, some Member States (14) opted for a centralised approach designating a single national authority for DSPs, OESs, and as a SPOC, while others (14 Member States) have decided to designate several sectoral authorities to coordinate their actions.<sup>177</sup>

Before the NIS Directive came into force not all the Member States had a CSIRT in place. Nowadays, all Member States have at least one or even more (sectorial) CSIRTs<sup>178</sup> and have to ensure that these CSIRTs have adequate resources to effectively carry out their tasks under the Directive. More than 90 percent of all national CSIRTs or government teams with national scope reached the basic maturity level, averagely being close to reaching the intermediate maturity level<sup>179</sup>.

Some Member States have fostered the development of fora where companies can exchange information about cybersecurity. This includes inter alia public private partnerships (PPPs) or sectorial Information Sharing and Analysis Centres (ISACs). In 2015 only five Member States had established formal PPPs for cybersecurity and in 2020 these partnerships are still lacking in eleven Member States. The below chart sums up the state of play of national capabilities among the 27 Member States and the UK:

---

<sup>175</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>176</sup> Bird & Bird (2020), Developments on NIS Directive in EU Member States and ENISA- (2020) National Cyber Security Strategies- Interactive Map. Available at: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map>

<sup>177</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>178</sup> ENISA (2019), Study on CSIRT landscape and IR capabilities in Europe 2025. Available at: <https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025> (last accessed on 16.05.2020).

<sup>179</sup> TI Accreditation was used as baseline for the Basic Maturity Level <https://www.trusted-introducer.org/processes/accreditation.html>



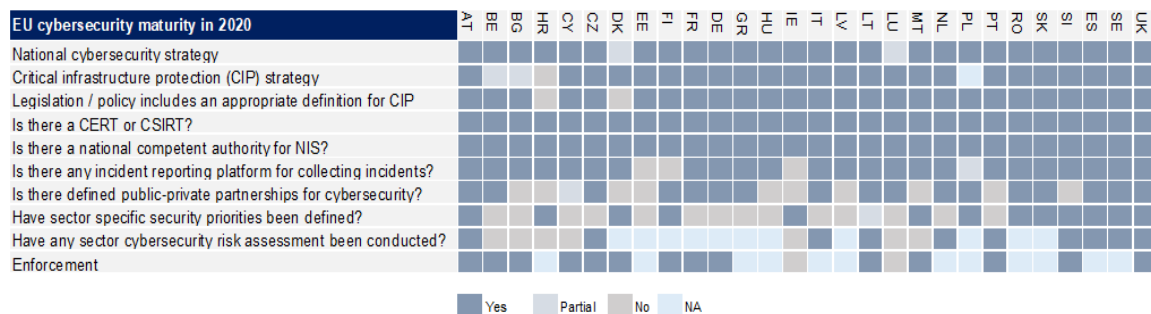


Figure 2 EU cybersecurity maturity in 2020<sup>180</sup>

Overall, during the evaluation, a lack of adequate financial resources and staffing emerged as one of the most relevant challenges that national competent authorities pointed out in the implementation of the NIS Directive. This is linked to the difficulty for national administrations to offer competitive salaries for highly skilled employees. In some Member States, no additional staff has been recruited. Instead, the available staff members have been tasked with the implementation of the NIS Directive in addition to their usual responsibilities.

### OES identification

The NIS Directive does not determine which companies will be included as OES under its scope. Instead, Article 5(2) sets out criteria that Member States will need to apply in order to carry out an identification process, which will ultimately determine which companies belonging to the type of entities under Annex II will be considered as OES and be subject to the NIS Directive. Annex II lists seven core economic sectors and their subsectors considered as essential for the effective functioning of the internal market: energy (electricity, oil, gas), transport (air, rail, water and road), banking, financial market infrastructures, health sector (including hospitals and private clinics), drinking water supply and distribution, and digital infrastructure (IXPs, DNS service providers and TLD name registers). These sectors have been chosen based on their potential vulnerabilities to threats and attacks, due to their high dependence on network and information systems and due to their essential role for the functioning of the internal market in the Union.

Member States have been given large room of discretion in selecting the relevant entities in order to account for national specificities.<sup>181</sup> In the absence of detailed guidance on how to identify OESs, Member States have developed a variety of *methodologies*,<sup>182</sup> also with regard to the definition of essential services and the setting of thresholds.<sup>183</sup> For example there are Member States, in which public authorities conduct the identification process (top-down identification) and Member States, in which operators were required

<sup>180</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report; based on BSA (2015), Bird & Bird (2020), ENISA (2020).

<sup>181</sup> COM (EU) 2019/546 final, Report From The Commission To The European Parliament And The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems (OES Report), 28.10.2019, Section. 1.1.3.

<sup>182</sup> OES Report, Section. 2.1.

<sup>183</sup> OES Report, Sections 2.1 and 2.3.



to verify themselves whether they meet the national criteria (self-identification).<sup>184</sup> One of the elements influencing national methodologies was the pre-existence of a framework on critical infrastructures or other national provisions on “vital operators”. In such cases, Member States used their prior experience as a point of reference and incorporated specificities related to the NIS Directive into existing methodologies. Differences in national methodologies fall in the following main categories: essential services, use of thresholds and their levels, degree of centralisation, authorities in charge of identification and assessment of network and information systems dependence.<sup>185</sup>

As regards the *definition of essential services*, Member States apply different levels of granularity: some provide a list of detailed services they consider essential, whereas other Member States indicate only general types of services leaving room for interpretation.<sup>186</sup> As concluded by the OES Report, this leads to consistency gaps, which renders it difficult to compare the lists of essential services and, more importantly may lead to fragmentation, if operators in one Member State are exposed to additional regulation while others providing similar services in another Member State are excluded.<sup>187</sup> The *numbers of services* identified also varies greatly between Member States. With an average of 35 services per Member State, the number of identified services ranges from 12 to 87, as shown in Figure 3 below.

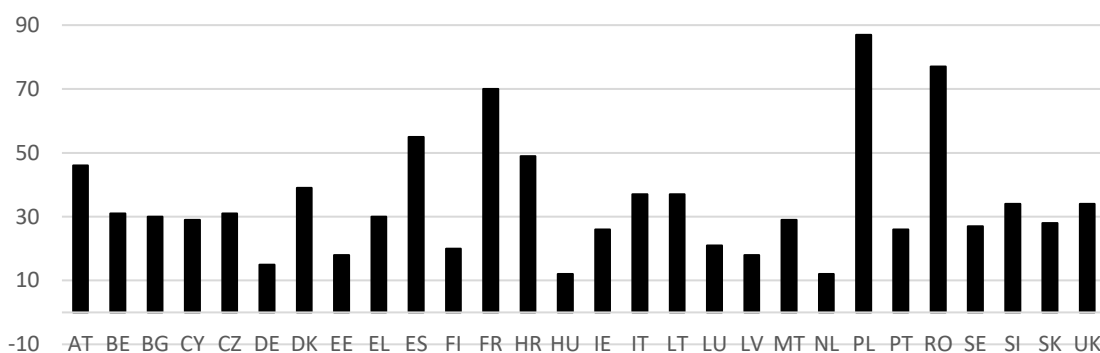


Figure 3: Overall number of essential services identified by Member States

Most Member States apply thresholds to identify OESs, which can be sector-specific or cross-sectoral and vary from Member State to Member State.<sup>188</sup> They may rely on a single quantitative factor, a larger set of quantitative factors or a combination of quantitative and qualitative factors.<sup>189</sup> The various approaches taken by Member States have ultimately led to very different result also in the number of identified operators in the sectors and subsectors.<sup>190</sup>

<sup>184</sup> OES Report, Section 2.1.

<sup>185</sup> OES Report, Section 2.1.

<sup>186</sup> OES Report, Section 2.2 taking the example of approaches chosen by Member States in the identification of essential services in the electricity subsector, where Estonia takes the least granular approach with ‘electricity supply’, whereas Bulgaria with the most granular approach enlist the ‘distribution of electricity’, ‘ensuring the functioning and maintenance of a distribution system for electrical energy’, transmission of electricity’, ‘operation, maintenance and development of an electricity transmission system’, ‘electricity production’ and ‘electricity market’.

<sup>187</sup> OES Report, Sec. 2.2.

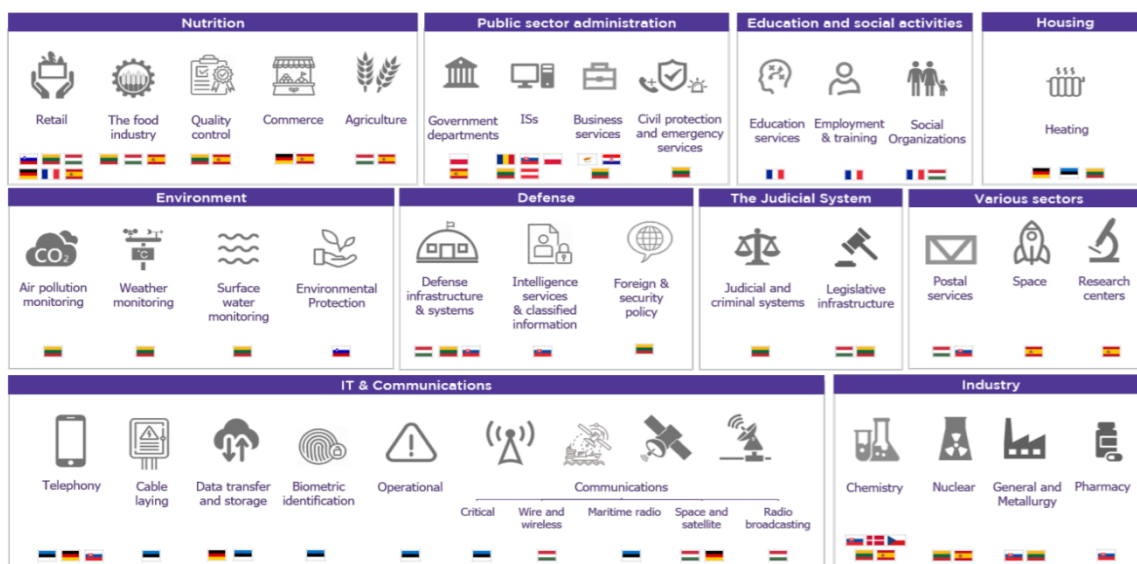
<sup>188</sup> OES Report, Section 2.3.

<sup>189</sup> OES Report, Section 2.3.

<sup>190</sup> OES Report, Section 2.4.

The minimum harmonisation approach of the NIS Directive allows Member States to consider in the implementation also services that are not provided by entities in the sectors included in Annex II. The OES Report reveals that to reinforce cybersecurity in other sectors that Member States consider nationally sensitive, 11 out of 28 Member States have identified essential services in additional sectors. This highlights that there might be other sectors that are critical for society and the economy and also potentially vulnerable to cyber-incidents that should be considered by the Directive<sup>191</sup> (See Figure 4 below).

Figure 4: Additional sectors and subsectors identified by Member State<sup>192</sup>



As regards the organization of competent authorities at a national level, there are different degrees of centralisation when it comes to the authorities responsible for defining essential services and identifying operators with some Member States nominating a single authority in some others more than one. In some cases, operators were identified by a competent authority or a CSIRTs while in other cases by primary legislation or even through self-assessment and self-identification.<sup>193</sup>

Another issue related to the identification of OES is the cross-border procedure under Article 5(4) requiring Member States to engage in consultation with each other before reaching a final identification decision. The Cooperation Group has issued a reference document in July 2018 in order to help Member States conduct proper cross-border consultations.<sup>194</sup> However, it appears that only very few national authorities have made use of this tool at all or at least in a comprehensive and consistent manner. Among the possible explanations could be the time that it took Member States to carry out the identification, the lack of secure channel for communication, the lack of common

<sup>191</sup> OES Report, Section 2.5.

<sup>192</sup> The NIS Directive, An Overview of Transposition In Europe For Operators Of Essential Services (OESs), June 2020, based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report..

<sup>193</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>194</sup> *Identification of Operators of Essential Services – Reference document on modalities of the consultation process in cases with cross-border impact*, Cooperation Group Publication 07/2018.

understanding of the cross-border consultation process or the large number of cross-border operators active across several Member States<sup>195</sup>.

Finally, there appears to be a level of inconsistency with regard to the application of the *lex specialis* principle of Article 1(7). While most Member States identified OES in the banking and financial markets sector, a few Member States have not done so based on the argument that operators are providing services covered by *lex specialis*.<sup>196</sup> Similarly, some Member States appear to have identified OES that should be regulated under the European Electronic Communications Code (EECC) and thus falling under the provision of Article 1(3).<sup>197</sup> Others have decided to completely exclude providers of electronic communications networks or services, which also supply digital infrastructure services from the scope of the NIS Directive and only apply the EECC.

### *Digital service providers*

The notion of “digital service” is defined as “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services” which is of the type listed in Annex III of the Directive (Article 4(5)). Contrary to OES, the list of digital services in Annex III is applied in a homogeneous way in the Member States by all providers under the scope of the Directive<sup>198</sup> (as opposed to being identified per each Member State as is the case for OES). The list is limited to three types of digital services as per Annex III: cloud computing services, online marketplace and online search engines, selected due to their significant criticality as assessed by the time of adoption in 2016.

While Member States are allowed to impose stricter security and notification requirements for OESs than those enshrined in the Directive, they are prohibited to do so for DSPs according to Article 3 and 16(10) of the NIS Directive (the so-called principle of “maximum harmonisation”). Moreover, national competent authorities can only supervise DSPs "ex-post", when an authority is provided with evidence that a company does not fulfil its obligations.

Because of their cross-border nature, DSPs are also subject to one single jurisdiction within the EU based on the Member State of their main establishment. Pursuant to Article 18 of the NIS Directive, a DSP shall be deemed to be under the jurisdiction of the Member State, in which it has its main establishment. It further specifies that the main establishment is where a company’s head office is located. However, the Directive does not provide a precise definition of what constitutes a main establishment or a head office. Competent authorities usually refer to the commercial register to determine the establishment of an entity. However, the information in the national commercial registers is often limited to a particular Member State. Especially in the case of DSPs, which mostly operate across borders and/or have several establishments in the Union, such registers do not contain sufficient information about parent and sister companies throughout the Union to determine the location of the company’s main establishment in the Union.

---

<sup>195</sup> OES Report, Section 2.6.

<sup>196</sup> OES Report, Section 2.7.

<sup>197</sup> OES Report, Section 2.7.

<sup>198</sup> Recital 57 of the NIS Directive.

When DSPs offering services in the Union have no establishment in any Member State, they are required to designate a representative in one of the Member States where the services are offered (Article 18 (2) of the NIS Directive). However, the provisions of the Directive do not require DSPs to inform the competent authority of the very Member State in which they have designated their representative. Therefore, Member States have limited knowledge regarding their own competence for specific DSPs.

Due to the reactive ex-post supervisory approach to DSPs<sup>199</sup>, competent authorities should only take action when provided with evidence that a DSP is not complying with the requirements of the Directive. Thus, there is no general obligation on the competent authority to supervise DSPs. As a result, national competent authorities are cautious in being proactive and contacting the DSPs in order to establish the precise country of jurisdiction. Moreover, while implementing the Directive, in view of often limited resources, national competent authorities tend to prioritize the identification of OES to an effort to understand which DSPs fall under their jurisdiction. This limited overview of competent authorities of the DSPs under their jurisdiction has been regarded as a major obstacle in the enforcement of the obligations towards DSPs.

All these elements of the so-called “light-touch” regulatory approach applied towards DSPs have been motivated primarily by the perception at the time of the adoption of the NIS Directive that cybersecurity incidents in DSPs presented a lower degree of risk to society and the internal market in comparison to OES. However, it can be observed that in the past years, and particularly since the COVID 19 crisis, the digital services are becoming vitally important for the society and the economy. Especially cloud services providers are providing more often services that may be considered critical for the operation of OES services but also serve as infrastructure to many other online services that citizens and the market rely on.

### *Security measures*

Article 14(1) imposes on Member States to ensure that OES, having regard to the state of the art, take appropriate and proportionate technical measures to manage the risk posed to the security of the network and information systems, which the organisations use in the provision of their services.

Member States have opted for very different approaches when designing their national law on security requirements for OES. For example, some countries such as Estonia, France and Romania have decided to include these security measures directly in their legislative texts (laws, decrees, orders or equivalent), whereas in Belgium there is a presumption that OES fulfil the requirements if they comply with, or even obtain, ISO/IEC 27001 certification. This certification specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. For some other Member States, which did not chose to specify the security measures in their laws or use a certification framework, national competent authorities published implementation guidance materials (e.g. Italy)<sup>200</sup>. The consequence is that security requirements show a

---

<sup>199</sup> See Article 17(1) and Recital 60 of the NIS Directive.

<sup>200</sup> Van Tieghem (2020), ‘The NIS Directive, An Overview of Transposition In Europe For Operators Of Essential Services (OESs)’, Risk Insight. Available at: <https://lu.wavestone.com/en/insight/nis-directive-transposition-operators-essential-services/>; Based on the interim findings of the NIS review

great variation across Member States from granular approaches setting a minimum length for passwords in the absence of two-factor authentication to more general requirements. Usually, they are set by secondary legislation and in some cases are sector-specific while in others follow general rules based on risk analysis and management. This variation in approaches and the diversity in types of measures could lead to an uneven level of preparedness to cybersecurity incidents across EU Member States. Additionally, this makes it complex for multinational companies to comply with the security measures across the EU.<sup>201</sup>

As regards DSPs, Article 16(1) requires Member States to ensure that DSPs identify and take appropriate and proportionate measures to manage the risks posed to the security of the network and information systems which the DSPs use for the provision of their services taking account of the state of the art and a number of elements prescribed by the Directive (the security of systems and facilities; incident handling; business continuity management; monitoring, auditing and testing; and compliance with international standards). These elements are further elaborated in the Commission Implementing Regulation (EU) 2018/151.<sup>202</sup> With regard to security requirements to DSPs, the Directive precludes Member States from imposing any further requirements, i.e. it provides for maximum harmonisation (Article 3 and Article 1(6) of the NIS Directive).

#### *Incident reporting*

Articles 14(3) and 16(3) require OES and DSPs respectively to notify without undue delay the competent authority or CSIRT of any incidents with a significant impact on the continuity of the essential service provided.

With regard to OES, the parameters for a substantial incident are listed in Article 14(4)<sup>203</sup>. The parameters concerning incidents with DSPs are mentioned in Article 16(4)<sup>204</sup> and further specified in the Commission Implementing Regulation EU 2018/151<sup>205</sup>.

---

study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>201</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>202</sup> Article 2 of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

<sup>203</sup> These parameters according to Article 14(3) are the number of users affected by the disruption of the essential service, the duration of the incident and the geographical spread with regard to the area affected by the incident.

<sup>204</sup> The parameters according to Article 16(3) are the number of users, the duration of the incident, the geographical spread, the extent of the disruption of the functioning of the service, the extent of the impact on economic and societal activities.

<sup>205</sup> Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

When it comes to incident notification, the differences across Member States increase even more due to the different values and roles played by the two variables characterising the incident reporting requirements: thresholds and modalities of reporting.

As far as *thresholds* are concerned, in some Member States they do not exist at all and in others they are extremely detailed and/or vary by sectors. The multitude of sectoral approaches reflect the variety of OES and corresponding business models but could provide an obstacle to a common regulatory approach in the EU and to the activity of cross-border operators.

Overall, hardly any incident in the past two years has attained one of the established thresholds and therefore very few incidents are being reported to the national competent authorities<sup>206</sup>. The NIS Cooperation Group recognises that a simple parameter to define the threshold imposed by the Directive, such as ‘number of users’ can mean different things to different types of providers, from simple clients of an electricity provider to potential patients of a hospital<sup>207</sup>. There is also a broad consensus that the thresholds are set too high to trigger the notification under the NIS Directive regime.<sup>208</sup> In few Member States voluntary reporting is envisaged and encouraged through, for instance, the reporting of near-misses<sup>209</sup>.

In terms of the *modalities* of the incident reporting, Member States have opted for different approaches such as the use of online platforms and portals, hotlines or email notifications.<sup>210</sup> The delay for reporting varies across the Member States from “without undue delay” or “immediately” to 24 hours and for the first written or follow-up report from 5 days to 4 weeks. OES and DSPs need to report the incidents to different authorities in the various Member States – for example to the central or sectorial CSIRTs, or national centralised or sectorial competent authorities. In many cases, companies need to report the same incident to several competent authorities within one Member State via several different templates on the basis of overlapping legal requirements.<sup>211</sup> This has been a serious point of concern for both national authorities and operators.

### *Supervision and enforcement*

Article 15 requires Member States to provide competent authorities with the necessary powers and means to supervise operators of essential services. It also lays down the main elements of the ex-ante supervision process operators of essential services are subject to. This process includes the requesting of information and documentation from the entities in question, the gathering of evidence of effective implementation of security policies and the issuing of binding instructions to operators to remedy deficiencies.

---

<sup>206</sup> According to the feedback from the national competent authorities during the NIS country visits.

<sup>207</sup> NIS Cooperation Group (2018), Reference Document on Incident Notification for Operators of Essential Services, CG Publication 02/2018. Available at [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53644](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644), p. 24.

<sup>208</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>209</sup> Such Member States are e.g. in Austria, Lithuania, Slovakia.

<sup>210</sup> For a full picture of the incident reporting modalities across all Member States, see final NIS review study report due by December 2020/January 2021, not yet submitted at the time of the writing of this report

<sup>211</sup> The NIS incident reporting obligations might come in some cases in addition to similar reporting obligations, such as e.g. under GDPR, PSD2, eIDAS.

During the NIS country visits, the Commission has observed that many Member States do not have formal requirements for operators of essential services to submit documentation of their security policies. In even fewer cases, competent authorities are systematically checking whether companies are complying with the NIS rules. In most Member States, national authorities tend to prioritize and promote a collaboration approach focused on cybersecurity awareness instead of audits.<sup>212</sup> Among the companies that the Commission interviewed during the NIS country visits, most companies that have undergone an audit, have launched the procedure by themselves and have done so for reasons not directly linked to the Directive.

When it comes to the supervision of DSPs, Article 17 requires Member States to ensure that competent authorities take ex-post supervisory measures once provided with evidence that a digital service provider does not meet the security requirements or has not notified of a reportable incident<sup>213</sup>. In addition, competent authorities do not have a full picture of the digital service providers falling under their jurisdiction (as explained in the section on *Digital service providers* above). Even though some of the Member States (such as e.g. Ireland or the Netherlands) are aware of the most relevant digital service providers within their jurisdiction, the lack of official ex ante information exchange between DSPs and competent authorities significantly impedes any effective supervision of these service providers.

In terms of *organisational structures*, apart from the constant role that CSIRTs play in all Member State to receive incident notifications and provide assistance when needed, Member States have opted for many different supervisory approaches. Some Member States have a unique national agency to be the competent authority for supervision and enforcement (France, Germany) while others have decided to have sectoral authorities (Spain, Italy, United-Kingdom) or both (Belgium). According to the national legislative transposition, the compliance audits are led by the competent authorities in some countries (Italy, Spain, France) which can decide to delegate it to a qualified third party (Germany, UK). In some others, the OES has the opportunity to directly select the auditor firm, as long as it is qualified by the competent authorities (Belgium, France).<sup>214</sup>

While Article 21 requires Member States to lay down penalties that are “effective, proportionate and dissuasive”, the Directive does not provide any guidance to Member States as to what is considered as effective and dissuasive. As a result, the level of maximum penalties varies greatly between the Member States, ranging from around 1.400 EUR to 5.000.000 EUR or certain percentages of the global annual turnover of undertakings, ranging from 0.5% to 5%. Some Member States have only sector-specific rules, with no specified levels of maximum penalties. The maximum penalties laid down in the national regulations transposing the Directive in most Member States are lower than the average penalty of around 100.000 EUR.<sup>215</sup> Finally, competent authorities have so far been reluctant to actually apply penalties. As a matter of fact, not a single case of a

---

<sup>212</sup> Based on feedback from national competent authorities received during the NIS country visits.

<sup>213</sup> Article 17, Recital 60 of the NIS Directive.

<sup>214</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>215</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.



penalty having been applied to a public or private entity has been brought to the attention of the European Commission at the time of writing of this report.

### *EU Cooperation – Cooperation Group, CSIRTs Network*

The EU Cooperation under the NIS Directive takes place at a strategic level within the NIS Cooperation Group and at an operation level, within the CSIRTs Network.

*The Cooperation Group*<sup>216</sup> is the guiding body in the implementation of the NIS Directive, which aims to facilitate strategic cooperation between Member States and sharing of information, experience and best practice relating to the security of network and information systems. The Group is composed of representatives of the Member States, ENISA and the Commission that also provides the secretariat.

According to Article 11, the Cooperation Group has among others, the following specific tasks: providing strategic guidance to the CSIRTs Network; exchanging best practice on information sharing on incidents, incident notification processes and risks; assisting Member States in building cybersecurity capacity, discussing capabilities and preparedness of Member States and of national cybersecurity strategies and CSIRTs; exchange of information and best practices on awareness-raising, training, research and development of network and information systems, exchanging best practices about the identification of operators of essential services by the Member States and in relation to cross-border dependencies.

The Cooperation Group, meets on a regular basis and is chaired by the respective Member State holding the Presidency of the Council of the EU<sup>217</sup>. The Cooperation Group carries out its tasks on the basis of biennial work programmes. The first Work Programme laid the ground towards shaping the working methods of the Group, building trust between Member States and coming up with the most urgent deliverables. In February 2020, the Cooperation Group adopted its Second Biennial Work Programme (2020-2022). Meanwhile, the Cooperation Group has established itself as a key forum and point of reference for policy discussion on cybersecurity within the EU. Besides the plenary sessions of the Cooperation Group, Member States representatives meet in 12 work streams, where they discuss specific topics such as the identification of OES, security requirements, incident reporting, cross-border dependencies, digital service providers and capacity building. Moreover, for three of the sectors under Annex II of the NIS Directive there are already dedicated work streams – energy, digital infrastructure and health. The Cooperation Group has provided the forum for discussing additional issues of relevance such as elections security and large-scale cyber incidents and crises (Blueprint)<sup>218</sup>. The NIS Cooperation Group provided also the forum for a dedicated working group on the cybersecurity of 5G networks, bringing together competent authorities in order to support and facilitate cooperation. It produced a joint EU risk

---

<sup>216</sup> See NIS Cooperation Group website <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

<sup>217</sup> See Article 2 of COMMISSION IMPLEMENTING DECISION (EU) 2017/179 of 1 February 2017 laying down procedural arrangements necessary for the functioning of the Cooperation Group pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0179&from=EN>

<sup>218</sup> COMMISSION RECOMMENDATION of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.



assessment, a toolbox of mitigating measures as well as a progress report on the 5G toolbox implementation.

Among the key outputs of the NIS Cooperation Group are non-binding guidelines to the EU Member States to allow effective and coherent implementation of the NIS Directive across the EU and to address wider cybersecurity policy issues. Since its establishment, the Group has published eight working documents<sup>219</sup> and it is in the process of reviewing and updating some of them. The Cooperation Group has had a crucial role in bringing national authorities closer and creating trust in matters, some of which have been considered close to national security.

*The CSIRTs Network* established by Article 12 is another form of EU cooperation. The CSIRTs Network's aim is to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation. The CSIRTs Network is composed of EU Member States' appointed CSIRTs and CERT-EU. ENISA is tasked to actively support the CSIRTs Network, provide the secretariat and support incident coordination upon request. The European Commission participates in the network as an observer.

The main tasks of the CSIRTs Network are to exchange information on services, operations and cooperation capabilities, share incident information, identify a coordinated response to an incident, provide support to Member States in addressing cross-border incidents, discuss other forms of cooperation linked to early warnings, discussing preparedness and capabilities of Member States and issuing guidelines. The CSIRTs Network has to report to and request guidance from the Cooperation Group.

The rules for the functioning of the CSIRTs Network are defined in its terms of reference. The activity encompasses three meetings per year and the everyday operational cooperation happens mostly using online tools. The activity of the CSIRTs Network is structured in various working groups (such as CyberWeather, Maturity, Standard Operational Procedures and Tools), as well as the participation to cybersecurity exercises organised every year. In line with the Blueprint Recommendation, the CSIRTs Network set out modalities for cooperation and exchange of information in Standard Operating Procedures. These envisage different levels of intensity of cooperation, based on the threats level across the EU, and facilitate a coordinated response to incidents.

The need to get over the different levels of maturity among the national CSIRTs by improving the operational cooperation and facilitating the sharing of information between the EU Member States' CSIRTs and across the EU, has been the focus of the MeliCERTes project developed with the financial support of the EU<sup>220</sup>. Its primary purpose was to facilitate cross-border cooperation encompassing data exchange between two or more CSIRTs based on the concept of trust circles i.e. ad hoc groups of CSIRTs which mutually agree on co-operation based on the concept of trust. MeliCERTes became operational in January 2019 and has been refinanced to advance the facility

---

<sup>219</sup> Available here: <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>

<sup>220</sup> Public tender on Connecting Europe facilities — cybersecurity digital service infrastructure — SMART 2015/1089SMART 2015/1089.

MeliCERTes (to develop MeliCERTes II) in accordance with the evolving needs of the CSIRTs in the EU<sup>221</sup>.

The improvement in the cooperation methods by the CSIRTs Network has been shown in times of crisis, such as COVID-19. The CSIRTs Network had two meetings per week at the beginning of the crisis and produced nine reports on different issues and coped overall very well with the new crisis situation offering advice to Member States and improving confidence and trust among its members<sup>222</sup>.

As regards the cooperation between the CSIRTs Network and the Cooperation Group, although Article 11(3)(a) prescribes a role of strategic guidance to the CSIRTs Network for the Cooperation Group, the collaboration between these two fora has been limited to reports by the CSIRTs Network to the Cooperation Group due every year and a half, and to an annual joint session organised back to back with one of the Cooperation Group plenary meetings.

According to ENISA, the creation of the CSIRTs Network, had a very positive impact in clarifying actors' role and responsibilities within the incident response process, improving its overall governance. However, the NIS Directive had an unequal effect from one country to another due to the different pre-existing maturity of Member States with regards to incident response<sup>223</sup>.

#### **d) METHOD**

##### **Short description of methodology**

The present evaluation aims to analyse the implementation and application of the Directive in each Member State according to a number of specific criteria set out in the Commission's Better Regulation Guidelines (relevance, coherence, effectiveness, efficiency, EU added value and sustainability). The evaluation covered all 27 Member States and the UK<sup>224</sup> and their implementation of the Directive since the deadline for its transposition in May 2018.

The consultation activities aimed at collecting the views of Member States' competent authorities, Union bodies dealing with cybersecurity, operators of essential services, digital services providers, companies in other vulnerable sectors outside the scope of the current NIS Directive, trade associations, researchers and academia, cybersecurity industry professionals, consumer organisations and citizens. During the 27 NIS country

---

<sup>221</sup> See MeliCERTes <https://ec.europa.eu/digital-single-market/en/news/call-tender-advance-melicertes-facility-used-csirts-eu-cooperate-and-exchange-information>. The existing MeliCERTes version is using open source tools developed and maintained by CSIRTs. It allows for the use of any key functions undertaken by the CSIRTs, such as incident management, threat intelligence (encompassing event management, vulnerability management and threat management), secure communications and artefact analysis.

<sup>222</sup> Contractor's interviews with members of the CSIRTs Network. Reference is made especially to the cyber-attacks on hospitals in the beginning of the COVID-19 crisis. Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>223</sup> ENISA (2019), EU MS Incident Response Development Status Report. <https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report>.

<sup>224</sup> No country visit to the UK took place. The evaluation of the impact of the NIS Directive on the UK was mainly based on desk research.

visits, the Commission interviewed the 117 SPOCs, CSIRTs and national competent authorities, 136 OES and 18 DSPs.

In addition to the NIS country visits, which were carried out from June 2019 until July 2020, and the OES Report, the Commission published the NIS Directive review roadmap on 25 June 2020, which was open for feedback until 13 August 2020 and received 42 contributions. From 7 July until 2 October, the Commission held an open public consultation on the NIS Directive review with the general public.

The Commission received 209 stakeholders' replies via the official EU Survey channel. Beside the regular discussion on the implementation of the NIS Directive in the framework of the Cooperation Group and its work streams, the NIS review was discussed at 3 Cooperation Group plenary meetings at the time of writing of the present Report. In addition, the Commission received written contributions from ENISA and from 16 Member States authorities.

Assisted by the external contractor (a consortium of ICF, Wavestone and CEPS), the Commission also collected evidence via desk research, targeted surveys to the different stakeholder groups, 16 expert interviews, 4 workshops with experts and with representatives of national authorities of Member States and businesses in the relevant sectors under scrutiny, as well as other stakeholders. 46 national competent authorities from 24 Member States, 49 OES and 9 DSPs replied to the targeted surveys.

A more detailed presentation of the consultation process is described in the Summary report of the Open Public Consultation (see Annex 2 to the Impact Assessment Report).

### **Deviations from the Roadmap**

The inception impact assessment/roadmap for this initiative, which was published in June 2020 indicated that three regional workshops would be organised gathering Member States, representatives of competent authorities, operators and cybersecurity experts in the third quarter of 2020. However, due to the persisting measures to attenuate the impact of the COVID 19 crisis, these workshops were carried out in a virtual format as webinars. This allowed for a broader than regional participation in each of the workshops. The first workshop took place in June 2020 and drew the attention to the NIS Directive review process and its timing. The attendance was between 80 and over 100 participants respectively for the two sessions, the most active of them coming from national competent authorities.

During the second workshop in July 2020 (attended by over 90 participants), the focus was largely on the shortcomings of the current NIS Directive and improvement ideas. This workshop was well attended also by operators and digital service providers, which actively represented the views of the private sector.

Two Closing Workshops took place on 12 October (for competent authorities, gathering over 65 participants), and 13 October 2020 (for the private sector, gathering over 60 participants). These workshops aimed to engage in a reflection on potential policy options to further enhance the level of protection of network and information systems across Europe and their respective economic, environmental and social impacts accounting for current and future technological developments.

## **Limitations and robustness of findings**

Despite the extensive consultation activities with stakeholders and the open public consultation, there are a number of issues that have affected the robustness of the findings. Such are:

A lack of available evidence, including historical data, and low quality of information in some cases prevented a quantitative analysis of the changes introduced by the NIS Directive. For example, only few stakeholders provided quantitative data on costs and benefits of implementing the NIS Directive, and this made it difficult to quantify and monetise such impact measures (rather than to other aspects of the evaluation). As a result, the evaluation has relied mainly on stakeholder consultations.

The partial contributions to the online surveys by the Member States (responses covered 22 EU countries) prevented a fully-fledged comparative analysis across the European Union;

Relatively low response rate from DSPs (including micro and small businesses) in all consultation activities, which may result from the ‘light touch approach’ and ex-post supervision towards DSPs. Besides that, as observed during the in-depth interviews with different stakeholders, as DSPs are already complying with several international standards and certifications and they remain free to take the measures that they deem appropriate, they may see the need to comply with the NIS Directive as less relevant.

Limited evidence on the actual impacts of the Directive, since the Directive has been implemented by the Member States only as of 2018, and some of them have experienced delays in its implementation. At the same time, the risk of drawing invalid conclusions has been mitigated by the online surveys and in-depth interviews with national competent authorities, SPOCs and CSIRTs.

The above-mentioned issues limited the analysis especially in relation to the ‘EU added-value’, ‘effectiveness’ and ‘efficiency’ evaluation criteria. However, conclusions have been drawn based on the triangulation and validation of findings from desk research and the consultation activities with stakeholders against the different evaluation criteria.<sup>225</sup>

### **e) ANALYSIS AND ANSWERS TO THE EVALUATION QUESTIONS**

By comparing the baseline situation with the implementation state of play, it is possible to study to what extent the outputs and outcomes that can be observed (see the intervention logic described in *Figure 1* above) correspond to the expectations concerning what the Directive should achieve, i.e. a high common level of security of network and information systems within the European Union. The below analysis is based on the five evaluation criteria: relevance, EU added value, coherence, effectiveness and efficiency.

#### **Relevance**

The evaluation criterion of relevance assesses how the objectives of an EU intervention correspond to the current needs and problems in society, as well as to the wider EU policy priorities. Under this criterion, the analysis should identify if there is any

---

<sup>225</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

mismatch between the objectives of the intervention and the needs or problems, e.g. incorrect assumptions or any change in the circumstances.

As laid down in Article 1(1), the overall aim of this legislation is to achieve a high common level of security of network and information systems within the European Union so as to foster trust and cooperation among the Member States and improve the functioning of the internal market. This translates into several specific objectives. In addition to the objectives of setting out national frameworks and achieving cooperation at EU level, the analysis verifies whether all the relevant sectors and sub-sectors of OES as well as all types of DSPs that would be considered essential for the smooth functioning of the economy and society and covered under the scope of the Directive.

*Evaluation question:* To what extent are the original objectives of the NIS Directive still pertinent in relation to the evolving needs, technological advances and problems at both national and EU levels?

The results of the Commission consultations show that overall the specific objectives of the NIS Directive are relevant. Respondents consider as most relevant the objectives to take appropriate measures to prevent and minimise the impact of incidents (Article 14(2) and 16(2) and to take appropriate and proportionate measures to manage the cybersecurity risks (Article 14(1) and Article 16(1)). Also very relevant are the objectives to improve strategic cooperation and the exchange of information among Member States (Article 1(2b), Articles 11 and 12) and adopt a NIS strategy and notify significant incidents. NCAs find it relevant to contribute to the development of trust and confidence between Member States and to set up inter-institutional cooperation at national level to fulfil the obligations under the Directive.

Operators of essential services, DSPs and NCAs believe that the issues, which were considered most prominent at the time of adoption of the NIS Directive are still very relevant until today. Such are the increasing magnitude, frequency and impact of cybersecurity attacks and incidents, which could cause major damage to the economy of the Union, the insufficient capabilities in the Member States and different preparedness, leading to fragmented approaches across the EU.

However, the growing interconnectedness and the changing threat landscape also resulted in legal gaps and uncertainties stemming, among others, from the implementation of the Directive at national level. The inconsistencies in the national implementations of the Directive put in question the achievement of a level playing field for some operators within the Internal Market.

For instance, as explained above in Section c) on implementation (OES identification), there is a considerable lack of harmonisation across the Union when it comes to the identification of OES. Stakeholders agree that the minimum harmonisation approach towards OES leaving an important degree of flexibility to Member States in the transposition and thus leading to very diverse results, is one of the key shortcomings of the NIS Directive. The result is a misalignment of security requirements and incident notification requirements for OES across Member States.

The minimum harmonization approach also led to the inclusion of additional sectors and corresponding sub-sectors beyond the scope of the Directive considered nationally sensitive and potentially vulnerable to cyber-incidents. The consultation confirmed that most NCAs believe that the Annex II of the NIS Directive does not cover all relevant

sectors and subsectors when it comes to the provision of services essential for the economy and society as a whole.<sup>226</sup> For instance, the majority of the competent authorities judged (“to a great extent”) that the sectors electricity generation, wastewater, emergency services, food supply and public administration could be added.

Also, due to the significant interdependencies with the other sectors under the NIS Directive, the telecoms sector, currently regulated under the European Electronic Communications Code (EECC), is considered as meriting to be part of the scope of the NIS Directive, to ensure coherence and consistency with the NIS Directive provisions.

Comparing the NIS Directive objectives and the current needs and problems in the area of cybersecurity within the EU, there are new challenges coming from the evolving digital transformation of our society. In view of the growing interconnectedness and interdependencies between sectors and providers, according to a majority of OES, the main criteria to identify emerging essential sectors and/or services that need to fall within the scope of the Directive are the reliance on the respective sector or service of other essential sectors (or a number of essential services) expressly mentioned within the scope of the Directive.<sup>227</sup> This leads to the need for introducing policies related to supply chain cybersecurity management. The increasingly connected ICT infrastructures, the rising number of connected devices through IoT and industry 4.0, the growth of 5G networks raise concerns regarding vulnerabilities in the supply chain could have cascading impacts across multiple critical infrastructures and services.

Regarding DSPs, the open public consultation showed that there was no agreement among stakeholders whether Annex III of the NIS Directive covers all relevant types of digital services, as around a third of respondents disagreed while 26.7% ‘agreed’ with the statement. The agreement varied also considerably between the groups, with agreement ranging from only 14.3% (NCAs) to 50% (Citizens). More generally, a third of the operators and DSPs believe there is insufficient consideration of critical internet-related technologies/entities (e.g. data centres and content delivery network (CDN) or geolocation services, social media platforms are not covered), which may render the entire digital ecosystem vulnerable. The majority of NCAs consider as a main shortcoming the limitations in determining the DSPs falling under the scope of the Directive, the light-touch approach when it comes to supervision of security measures and incident reporting, as well as the insufficient clarity about the establishment of jurisdiction for DSPs. Incident reporting as a result of high thresholds and the enforcement measures are also considered as insufficient and are also subject to criticism by the NCAs.<sup>228</sup> The limited information sharing between Member States, potentially hampering the effective handling and prevention of incidents, a misalignment of security requirements for operators of essential services across Member States, insufficient voluntary incident reporting schemes are among the other main identified shortcomings.

---

<sup>226</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>227</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>228</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

## Coherence

This criterion investigates how different actions of the NIS Directive fit together and within a wider framework (e.g. other EU initiatives). The analysis of *external coherence* highlights areas where there are synergies or tensions among different EU interventions. Meanwhile, the analysis on *internal coherence* evaluates how the various elements of the Directive work together in order to achieve its objectives<sup>229</sup>.

*Evaluation question:* To what extent does the NIS Directive fit well within the wider EU cybersecurity policy, and, more specifically, is it coherent with other EU interventions in the field of cybersecurity (incl. in specific sectors or with regard to security of products) and critical infrastructure protection?

For this analysis, the evaluation looked into the different definitions and concepts provided by the NIS Directive and analysed how these are coherent to other EU interventions such as Directive (EU) 2018/1972 (EECC)<sup>230</sup>; Directive 2008/114/EC (ECI Directive)<sup>231</sup>; Directive 2015/2366/EU (PSD 2)<sup>232</sup>; Regulation (EU) 2019/881 (Cybersecurity Act)<sup>233</sup>; Regulation (EU) No 910/2014 (eIDAS Regulation)<sup>234</sup>; and Regulation 2016/679 (GDPR)<sup>235</sup>. The analysis revealed that there should be a better alignment of requirements (e.g. reporting authorities, thresholds, time-frame, and penalties), between the NIS Directive and other EU legislation, especially considering risks such as double jeopardy (e.g. imposition of administrative fines under different regimes in case of non-compliance). For instance, there are overlapping reporting obligations with the GDPR since, while many security incidents involve some personal data, the relation between the two instruments – NIS Directive and GDPR - is not explicitly clarified. Moreover, conflicting reporting obligations with the eIDAS Regulation may arise when digital certificates are used for authentication in services that fall under the scope of the NIS Directive, while duplicated reporting schemes exist with PSD2<sup>236</sup> as payment service providers shall report operational or security incidents to

---

<sup>229</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)

<sup>230</sup> Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, pp. 36-214.

<sup>231</sup> Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, pp. 75-82.

<sup>232</sup> Directive (EU) of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, pp. 35-127.

<sup>233</sup> Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013, OJ L 151, 07.06.2019, pp. 15-69.

<sup>234</sup> Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OF L 257, 28.08.2014, pp. 73-114.

<sup>235</sup> Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016, pp. 1-88.

<sup>236</sup> The Commission Proposal for a Regulation on Digital Operational Resilience for the Financial Sector or the Digital Operational Resilience Act (DORA) adopted on 24 September 2020 amending PSD2

their competent authorities and to their respective NIS competent authority as well. The different reporting schemes that overlap however usually have different aims, thresholds and requirements, and therefore are not substitutable. As such, the findings from the coherence analysis suggests that instead of benefitting from synergies by identical requirements, different reporting mechanisms may hamper the aims of these instruments.<sup>237</sup>

Furthermore, the NIS Directive presents a number of legal concepts, which allow for interpretation and so provide large room for manoeuvre to Member States to decide how to reach a high level of security of network and information systems. For example, the definitions of ‘significant’ or ‘substantial’ effect; ‘appropriate and proportionated technical and organisational measures to manage the risks’ are not precisely elaborated in the Directive. Although the majority of stakeholders replying to the online surveys declared that the concepts and definitions provided in the NIS Directive are clear enough, respondents flagged that the identification of OES and definition of DSPs are the main unclear points of the Directive and could impact the level of awareness of their obligations including insufficient clarity of the provisions on how to determine the ‘significance of the impact of an incident’. They mentioned that more clarity regarding provisions on ‘incident notification’ and ‘reporting requirements’ would be welcome. Lastly, while the Directive aims to achieve a high ‘common’ level of security of network and information systems’, it set minimum standards by legal concepts such as ‘state of the art’, ‘appropriate technical and organisational measures’, ‘effective, proportionate and dissuasive’ penalties, thus leaving room for various national interpretations risking to achieve diverging standards.

Finally, the information gathered indicates that the NIS Directive has made a positive contribution to the establishment of a common high level of security of network and information systems and thus upscaling capacities, cooperation and risk management practices across the EU Member States. Prior to its adoption, there was no regulation for cybersecurity in some Member States, yet all of them are now complying with the minimum requirements imposed by the NIS Directive. However, evidence suggests that there are significant discrepancies in the obligations imposed on OES, as well as in the enforcement of the Directive across Member States, and uncertainty about scope and jurisdiction for DSPs. This suggests that a sufficient level playing field particularly important for cross-border operators, has not yet been achieved.<sup>238</sup>

### **EU Added Value**

This criterion investigates the changes of the EU intervention compared to what could reasonably have been expected from national and regional actions<sup>239</sup>.

*Evaluation question:* What has been the added value of the NIS Directive compared to what could have been achieved by Member States at national or regional level?

---

aims at streamlining incident reporting obligations for the financial sector among other things. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A595%3AFIN>

<sup>237</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>238</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>239</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)



The evidence suggests<sup>240</sup> that the Directive has played an important role in creating a cybersecurity framework and, therefore, in overcoming concerns regarding national sovereignty in this domain by strengthening the security of network and information systems across the Union without hindering or prejudicing the respect of the subsidiarity and proportionality principles.

There was an increase in the number of national cybersecurity strategies across the EU Member States since the implementation of the NIS Directive. The reliability and security of network and information systems directly contributes to the overall functioning of the Internal Market. This is one of the main priorities of the EU (Article 114, TFEU), and without a harmonised set of cybersecurity rules at EU level, it is unlikely that improvement in cybersecurity capacity and preparedness would be achieved in the Member States.

Nonetheless, the consulted stakeholders confirmed that there is room for improvement in the provisions of the NIS Directive in relation to the creation of a more coherent cybersecurity framework across the Union. There is the need to harmonise the Member States' methodologies to identify OESs, their definition, and the incident thresholds, as asymmetries in relation to OESs dispositions create a risk of fragmentation in the internal market. Similarly, it appears that a certain degree of inconsistency exists in the national application of the Directive with regard to Article 1(3) leading to the identification of OESs where sector-specific rules apply (e.g. in the telecoms sector) and insufficient OES identification in some of the sectors listed in Annex II. The role of the NIS Cooperation Group could also be strengthened to promote a common understanding on how to coherently implement the Directive amongst Member States.<sup>241</sup>

Overall, the implementation of the Directive allowed Member States to enjoy a series of direct and indirect benefits, such as increased safety for all stakeholders, increased information sharing, increased information availability, among others. However, when comparing challenges at the time of the NIS Directive adoption and current and future issues and threats, further EU action is and will be required. Among the most pressing upcoming challenges are (i) the necessary development of cybersecurity skills in the EU; (ii) the need of cybersecurity standardisation efforts; (iii) the necessity to pursue EU efforts to strengthen incident response capabilities, procedures, processes and tools to avoid eventual repetitions or loopholes; (iv) and the consolidation, planning and work ahead on EU capabilities to ensure cybersecurity resilience of current and upcoming technologies (e.g. 5G networks, artificial intelligence, internet of things, blockchain).

To sum up, the NIS Directive has contributed to the achievement of results that could not have been attained at the national level. In this sense, the continuation of the EU action is needed to further ensure a high common level of security of network and information systems across the Union for the European society and its citizens.<sup>242</sup>

---

<sup>240</sup> E.g. 57% of the Competent Authorities agree 'to a great extent' on the fact that the NIS Directive improved cooperation and the exchange of information among Member States.

<sup>241</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>242</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

## **Effectiveness**

This criterion intends to (i) assess the extent to which the general and specific objectives of the NIS Directive have been achieved; (ii) identify any significant factors that may have contributed to, or inhibited progress towards, meeting these objectives; and (iii) investigate any negative or positive changes produced beyond the intended effects of the NIS Directive<sup>243</sup>.

*Evaluation question:* To what extent and why has the NIS Directive been an effective instrument for achieving a high common level of security of networks and information systems within the EU?

Evidence indicates that the full transposition of the Directive by Member States has generally improved the situation of EU cybersecurity. As observed, stakeholders agree that both the adoption of a national strategy and the designation of one or more national competent authorities, CSIRTs and of a SPOC were effective in achieving a higher level of security of network and information systems. The adoption of the national cybersecurity strategies gave impetus to the implementation of a series of concrete policy actions such as the definition of a risk-assessment plan, a governance framework to achieve the objectives of the national strategy and the identification of measures related to cybersecurity capacity building such as preparedness, response and recovery. This legal provision helped the countries with less capacity to make a substantial step forward in cybersecurity preparedness, ensuring a high level of security in their territory.

However, shortcomings in the implementation may hinder the full achievement of the objectives and expected results of the NIS Directive. For instance, significant differences remain concerning the implementation of risk assessment procedures, the availability of reporting platforms for incidents and the allocation of resources and staffing to designated national competent authorities.

Differences also exist among Member States with respect to the designation of competences at the national level (e.g. centralised vs. decentralised approach). Moreover, there are significant divergences in the ability of competent authorities to accomplish their tasks due to different levels of allocation of adequate financial and human resources. Most stakeholders that took part in the consultation agree that the lack of adequate financial resources and staffing emerged as one of the most relevant challenges that national competent authorities have faced in the implementation of the NIS Directive.

As far as the effectiveness of the Directive in fostering CSIRTs ability to comply with requirements and tasks is concerned, the evaluation shows that although a minimum maturity level was met, the level of operational capacity and reliability of national CSIRTs also greatly varies. In this respect, resources' limitation or lack of technical capacity may create challenges for CSIRTs to meet all the responsibilities defined in Annex I of the NIS Directive while having to deal with incidents of national priority. National CSIRTs are not always considered to lead in raising awareness on threats among the private sector. Instead, operators often turn to commercial organisations providing early warning and incident response capabilities. Finally, because the role and

---

<sup>243</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)

range of national CSIRTs diverges, their cooperation with national law enforcement, the SPOC, other competent authorities, OES and DSPs have also been uneven. According to the OES' responding to the online survey, the main challenges faced when cooperating with the national competent authorities and national CSIRTs are related to the lack of understanding about their field of activity, the focus on national critical infrastructure rather than cross-border dependencies, and the lack of support for information sharing, such as a mechanism for authorities to share information with established private sector initiatives under public-private partnership programmes (see above in Section on *Implementing and transposing measures*).<sup>244</sup>

Regarding the effectiveness of SPOCs in fulfilling their tasks as members of the wider national institutional cybersecurity framework, most respondents considered that SPOCs are effective in coordinating issues related to the security of network and information systems and cross-border cooperation at Union level. However, some stakeholders believe that SPOCs and CSIRTs tasks are overlapping in some Member States and therefore the liaison function of these entities should be clarified. Respondents also explained that SPOCs should be given more responsibilities than just transmitting information between different stakeholders. They also pointed out that it is common that important information is missed or not distributed correctly. A high number of competent authorities' respondents declared that they have limited overview over the level of cooperation between NCAs and SPOCs in another Member State.

With respect to the effectiveness of cooperation at the EU level, while the Cooperation Group has facilitated the exchange of information and has offered guidance for Member States consultation in cases of OES operating across borders, few members actually use the cross-border consultation instrument. The evaluation also shows the need for more structured cooperation and improved communication between the Cooperation Group and the CSIRTs Network.

Another important factor which stood in the way of fully achieving the NIS Directive objectives is the variation in methodologies to approach the definition of essential services, the identification of OES, and the specification of thresholds. These discrepancies hinder the management of cyber-dependencies for OES operating across different Member States limiting the effectiveness of the NIS Directive and raising concerns about the proper enforcement at national level and the consistent implementation of cybersecurity measures across the EU.

The evaluation also analysed the Member States' ability to establish security requirements and to impose incident reporting requirements on OES and DSPs.

Minimum-security requirements vary across Member States, ranging from setting a minimum length for passwords in absence of two-factor authentication to more general requirements. In this respect, there is the need to define similar security objectives for each sector, especially for OES with cross-border activities, and to consider specific measures by market-operators of different size, especially SMEs.

With regard to incident reporting requirements, the differentiation in schemes is not optimal for cross-border providers, which are often subject to different notification

---

<sup>244</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

regimes. Also, under the current reporting regime, cybersecurity authorities are unable to acquire knowledge relative to incidents below a certain threshold. Indeed, only in few Member States voluntary reporting is envisaged and encouraged through, for instance, reporting near misses. In order to promote incident reporting it is thus necessary to streamline the definition of a significant incident and /or to adjust thresholds.

Thresholds and modalities of reporting vary substantially across Member States. It can be observed that in some countries thresholds do not exist at all while in some others they are extremely detailed and/or vary by sectors. Such multitude of sectoral approaches challenge a common regulatory approach in the EU and hamper the activity of cross-border operators.

In relation to the effectiveness of the NIS Directive regarding DSPs, a majority of the limited number of DSP respondents<sup>245</sup> consider that it has been effective in achieving its overall objectives. At the same time, the majority of national competent authorities<sup>246</sup> consider as ineffective the approach for determining the DSPs falling under the scope of the Directive stemming among others from an insufficient clarity about the establishment of jurisdiction for DSPs, as well as the ineffective light-touch approach when it comes to supervision of security measures and incident reporting. Another criticism by national competent authorities is that, as a result of high incident reporting thresholds, very few incidents are being reported, also failing to meet the set objectives.

Finally, with respect to penalties, there is great variation in magnitude across Member States and their application. Penalties vary by sector, by entity, by type of incident, among others. The effectiveness and dissuasiveness of some of the maximum penalties provided for in some Member States is also questionable. Moreover, Member States to date have never applied any type of penalties. This situation clearly calls for a specific intervention to align the penalties across Member States.<sup>247</sup>

### **Efficiency**

This criterion considers the relation between the resources used by the intervention and the changes that it generated. Under this criterion, the analysis looks at the costs and benefits of the EU intervention as they accrue to different stakeholders to evaluate whether the benefits are achieved at a reasonable cost and the costs are proportionate to the benefits.<sup>248</sup>

*Evaluation question:* To what extent have the effects of the NIS Directive been achieved at a reasonable cost?

The results of the targeted consultation activities concerning the costs and benefits of the NIS Directive have highlighted a lack of quantitative data. The missing estimates of costs and benefits is due to four main reasons: (i) data are not available as the Directive has only recently been implemented; (ii) the reluctance of stakeholders to share such data, (iii) the difficulty in attributing the costs and benefits of new cybersecurity measures

---

<sup>245</sup> Overall 9 DSPs (including trade associations) replied to the targeted survey and 16 DSPs (including 3 trade associations) replied to the Open Public Consultation.

<sup>246</sup> 46 NCAs replied to the targeted survey and 14 NCAs replied to the Open Public Consultation.

<sup>247</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

<sup>248</sup> Better Regulation Tool#47 on Evaluation Criteria And Questions. Available at: [https://ec.europa.eu/info/sites/info/files/file\\_import/better-regulation-toolbox-47\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-47_en_0.pdf)

directly to the NIS Directive, and (iv) the non-easily quantifiable costs and benefits, such as the reduced number of cybersecurity incidents or the increased compliance costs.

Despite the lack of estimates that equally concerns costs and benefits, it is possible to draw some partial conclusions. Analysing the findings of the targeted consultations related to the costs coming from the NIS Directive, it is evident that the respondents have expressed common views, reporting that they did not incur significant operational, administrative, and compliance costs. The costs that the respondents flagged as the most relevant are compliance costs and, in particular, the duplication of efforts and the time invested to comply with different European legislation, imposing different reporting obligations to different authorities, timelines, and criteria. However, the duplication of reporting requirements due to the lack of external coherence cannot be reported as a direct cost of the NIS Directive.

In regard to the benefits, the results of the targeted consultation activities show that the respondents have experienced additional benefits coming from the NIS Directive, such as the improved security for the functioning of economy and society and the increased trust and cooperation among the Member States. The perceived benefits vary across stakeholders. Competent authorities gave mainly positive replies in relation to the benefits coming from the NIS Directive, while OES and DSPs experienced one main benefit - a reduced impact of cybersecurity incidents for OES, and increased trust in the digital economy and the internal market for DSPs. However OES and DSPs were more critical in relation to other types of benefits, i.e. decreased costs of security incidents, including malicious attacks and a reduced number of NIS incidents.

Finally, the respondents' answers concerning the proportionality of the costs and benefits of the NIS Directive are positive, with all stakeholder groups considering the cost proportionate to the benefits to a great or to a moderate extent. The stakeholder group that is more critical about the proportionality of costs and benefits is the OES in the banking and financial market infrastructure sectors. This is partly due to the fact that entities in these two sectors considered themselves already compliant with requirements similar to those imposed by the Directive before the entry into force of the NIS Directive.

Overall, the results of the consultation activities tend to show that the costs of the Directive are reasonable and proportionate to the benefits achieved. However, no conclusive consideration can be done in relation to the costs and benefits, as the lack of estimates limits the analysis of the efficiency of the NIS Directive.<sup>249</sup>

## **f) CONCLUSIONS**

Overall, the NIS Directive can be considered as a major first step in reaching the objectives to raise the common level of cybersecurity amongst the Member States. The NIS Directive has ensured the completion of national frameworks by defining the national cybersecurity strategies, establishing national capabilities and implementing regulatory measures covering the critical infrastructures and actors identified by each Member State. The Directive has also greatly contributed to developing the cooperation at the EU level within the frameworks of the Cooperation Group and CSIRTs Network.

---

<sup>249</sup> Based on the interim findings of the NIS review study to be included in its final report due by December 2020/January 2021, not yet submitted at the time of the writing of this report.

However, the growing interconnectedness and dependence on digital technologies as well as the expanding threat landscape have intensified the need for a strong EU response. Member States capabilities are still unequal and resources are often insufficient leaving certain competent authorities in a position, in which they can no longer effectively fulfil their obligations under the Directive. In view of the minimum harmonization requirements imposed by the Directive, Member States have taken diverging approaches when identifying OES and prescribing security requirements and incident reporting obligations. This has led to discrepancies and gaps in the implementation of the Directive and has failed to achieve a sufficient level playing field for operators and in particular cross-border players, within the Union. The sectors identified beyond the scope of the Directive also demonstrate the need to expand the scope to further sectors that are considered essential and equally vulnerable to cyber threats. In view of DSPs' increasing role in the digital economy, the current light-touch regime, which has demonstrated its limitations, merits a re-evaluation and a clarification regarding the type of providers that fall in the scope, the process to establish DSP's jurisdiction within the Union and the national competent authorities' ex-ante supervisory powers. Information sharing has remained limited both from operators and DSPs as between national competent authorities. The high incident reporting thresholds leading to only few reportable incidents stay in the way of developing a comprehensive view of the threat landscape. Despite the success of the Cooperation Group, due to the voluntary nature of information exchanges between the authorities, no systematic information sharing between Member States has been taking place. This is the case also in situations with direct cross-border implications. Therefore, to be able to keep in pace with technological and threat landscape evolution and to achieve the original objectives of the NIS Directive and make it future-proof, the discrepancies between the Member States transposition and legal gaps need to be removed.