EUROPEAN
COMMISSION

Brussels, 16.12.2020
SWD(2020) 345 final

PART 3/3

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

Proposal for a Directive of the European Parliament and of the Council

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

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

Table of Contents

Annex 6: Overview of selected results of the targeted surveys conducted by the NIS review study 5

Annex 7: Overview of related cybersecurity legal acts and policy measures 45

Annex 8: Overview of policy options 55

Annex 9: Cross-sector and cross border propagation of incidents 63

Annex 10: Extract from the interim results of the NIS review study on a modelling for costs and benefits 65

Annex 11: List of indicators to monitor high-level progress towards general objectives 67

Annex 12: List of indicators to monitor progress towards specific objectives 70

Glossary: acronyms

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

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

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

ANNEXES

Annex 6: Overview of selected results of the targeted surveys conducted by the NIS review study

Throughout July-September 2020, the NIS review study conducted targeted surveys for three categories of stakeholders: competent authorities, operators of essential services and digital service providers. The surveys had: 46 respondents on the side of competent authorities, 49 for operators of essential services and 9 for digital service providers.

This annex provides a summary of the results of the targeted surveys, as well as extracts of these results, as they were referred to throughout the impact assessment report. The results and charts were prepared by the Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) – N° 2020-665 – implemented by Wavestone, CEPS and ICF. The final report of the study, due by December 2020/January 2021 was not submitted at the time of the writing of this report.

Overview

The targeted consultation consisted of **online surveys** and **in-depth interviews**.

As part of the targeted consultation, the Project Team developed three **online surveys** targeting

- National Competent Authorities (CAs, including CSIRTs and SPOCs),
- Operators of Essential Services (OESs)
- Digital Service Providers (DSPs)

All three online surveys ran between 15 July and 4 September 2020. The questionnaires were tailored to each stakeholder group and were structured following the five evaluation criteria: relevance, effectiveness, efficiency, coherence EU added value.

The questions were grouped according to the main provisions of the NIS Directive exploring context specific aspects which gave the targeted respondent the possibility to provide evidence-based information coming from their experience.

The surveys prepared for OESs and DSPs were also shared with and disseminated through associations or networks of OESs and DSPs, significantly increasing the reach of the surveys through the snowballing technique.

The respondent breakdown was as follows:

Table 1: Overview of respondents to the targeted surveys

Respondent group	Total number of responses	Coverage
CAs (CSIRTs, SPOCs)	46	22 out of 27 MS + UK
OESs	49	All sectors in Annex II
DSPs	9	All services in Annex III

Source: Wavestone

In-depth interviews were conducted between 23 July 2020 and 8 September 2020. A total of 16 interviews were completed with the following stakeholders:

- 4 CAs

- 7 OESs
- 2 DSPs
- 2 EU Institutions and Agencies
- 1 Think-Tank

Contextual relevance

It was noted the increasing interconnectedness and reliance on digital infrastructures, technologies, and online systems, as well as resilience and trust in the supply chain made the NIS Directive all the more relevant in the current contextual settings. To illustrate this, 54% (25 out of 46) of the CAs responding to the targeted survey thought that the NIS Directive is relevant to a great extent in the current context.

The majority of OESs and DSPs respondents agree that all specific objectives of the NIS Directive are still relevant in the current contextual settings.

Across the groups (CAs, OESs, DSPs) the main issues identified with regard to the extent to which EU legislation on NIS still has relevance were:

- the increasing magnitude, frequency and impact of security incidents, and harmful actions;
- the unequal cybersecurity capabilities and preparedness in the Member States;
- the lack of common requirements for OESs and DSPs; and
- the insufficient structured cooperation among relevant actors.

Sectoral coverage

The targeted consultations confirmed that most CAs (31 out of 46, 67% of respondents) believe that the Annex II of the NIS Directive does not cover all relevant sectors and subsectors when it comes to the provision of services essential for the economy and society.

Unlike the CAs, the OESs shared mixed opinions as to whether to add sectors or sub-sectors to the Annex II of the NIS Directive (12 out of 49, 24% of respondents are in favour; 14 out of 49, 29% of respondents are not; and 23 out of 49, 47% do not know). For those who believe sector or sub-sectors could be added in addition to the ones identified by CAs, one additional sector was raised by OESs and is targeted at the elections service (authorities, technology and process) (5 out of 12, 42% of respondents agree 'to a great extent').

Emerging challenges

While there was overall agreement that the problems and needs that were considered most prominent when the NIS Directive was adopted are still relevant today and most likely require action at EU level. These problems led to the identification of a series of main needs in the legislation, including:

- implementing security measures to manage cybersecurity risks, and prevent, minimise and notify incidents;
- harmonising the identification process of OESs across the Member States; and
- addressing the ineffective approach for determining the DSPs falling under the scope of the Directive.

Coherence

Of the NIS Directive in the EU cybersecurity policy framework

The consultation covered the degree of coherence between the NIS Directive and a set of other EU legislative texts including: Directive (EU) 2018/1972 (EECC); Directive 2015/2366/EU (PSD2 Directive); Regulation (EU) No 910/2014 (eIDAS Regulation); Regulation 2016/679 (GDPR) ; and Regulation (EU) 2019/881 (Cybersecurity Act).

Across all three stakeholder groups, a significant share of the respondents could not pronounce themselves on the degree of coherence between the NIS Directive and other EU legislative texts. The remaining stakeholders consulted across the three groups noted a satisfactory degree of consistency of concepts and definitions between the Directive and the other EU instruments.

However, a better alignment among certain legal instruments could still be reached in relation to definitions, such as the notion of 'incident', as well as reporting requirements, which are heterogeneous in terms of reporting authorities, thresholds, timeframe, and penalties.

Of the NIS Directive concepts and provisions

The majority of CAs responding to the online survey (63%) indicated that the concepts and definitions provided in the NIS Directive are clear enough. However, 35% of the CA respondents held the opposite view and highlighted the definition and identification of OESs and DSPs as the main unclear points.

OESs and DSPs were also surveyed in order to gather their views on any potential clarity issues regarding the concepts and definitions provided within the NIS Directive. The majority of both (63% for OESs and 56% for DSPs) seem to consider concepts and definitions coming from the NIS Directive clear enough.

Overall, although the majority of the respondents to the targeted surveys declared that the definitions provided in the NIS Directive are clear enough, a number of legal concepts featuring in the NIS Directive were judged to entirely clear, e.g. definition of OESs and DSPs; 'significant' or 'substantial' impact and 'appropriate and proportionated technical and organisational measures to manage the risks'.

EU added value

Of the NIS Directive compared to Member States acting alone

According to the consulted CAs, the NIS Directive achieved results that could not have been achieved by national policies alone:

- 57% of the CAs responding to the online survey (26 out of 46) agreed 'to a great extent' on the fact that the NIS Directive improved cooperation and the exchange of information among Member States;
- 46% of the CAs (21 out of 46) also agreed 'to a great extent' that the Directive promoted effective operational cooperation through to the creation of a network of national CSIRTs; and
- 35% (16 out of 46) of the CAs agreed 'to a great extent' with the fact that the Directive guaranteed minimum capabilities and the establishment of a national framework.

Results for OESs and DSPs were more mixed regarding the added value of the NIS Directive regarding the above aspects. The most critical stakeholder group appeared to be the OESs taking part in the online survey:

- 29% (14 out of 49) of OESs only agreeing 'to a moderate extent' with the fact that the NIS Directive created a level playing field for OESs and DSPs across the EU, which could have not been achieved by national polices alone, in terms of security and notification requirements;
- 35% (17 out of 49) of OESs only agreed 'to some extent' with the effective implementation and enforcement of security requirements and notifications by OESs and DSPs.
- 41% of OESs (20 out of 49) indicated not knowing whether the NIS Directive improved cooperation and the exchange of information among Member States, and a further 35% (17 out of 49) indicated not knowing whether the creation of a network of national CSIRTs led to more effective operational cooperation.

Added value of the continuation of EU level action

Across the three stakeholder groups, responses showed that EU level action on NIS brings added value and should be continued when considering that:

- the general objective of the Directive is yet to be fully achieved;
- harmonisation between Member States, despite considerable efforts, remains incomplete, e.g. OESs identification;
- the revision of the NIS Directive is an opportunity to extend its scope to harmonise the EU landscape, e.g. supply chain security, new technologies, public-private partnerships.

Effectiveness

Achieving a high common level of security across the EU

Most of the CAs consulted in the targeted survey (92%, 44 out of 46) regarded either 'to a moderate' or 'to a great' extent to which the overall provisions of the NIS Directive were effective for achieving a high common level of security.

These results are corroborated by the relative majority of consulted OESs and DSPs, although they have shown more mixed opinions on the effectiveness of the Directive in achieving a high common level of security across the EU. In this context, it has been highlighted that while strategies and frameworks are now in place in all Member States, because of the fact that incident handling is different from Member State to Member State – especially in terms on methodologies, skills and practices –effective cooperation is extremely complex.

Enabling Member States to develop effective cybersecurity policies

The majority of CAs, OESs and DSPs positively assessed the effectiveness of the Directive in allocating power and tasks to national competent authorities, SPOCs and CSIRTs

While the NIS Directive was deemed across the three groups to contribute to the development of effective cybersecurity policies in the Member States, the results reveal that the level of at least some Member States' cyber maturity could still be improved.

Around two-thirds of the consulted CAs (30 out of 46) still consider at least to 'some extent' the insufficient capabilities in the Member States to ensure a high level of security of network and information systems to be relevant and continue to require action at EU level.

Security requirements/incident notifications for OESs & DSPs

The Directive was deemed to have contributed to OESs and DSPs effective management of risks posed to the security of network and information systems.

Results however show a need for improvement concerning:

- the misalignment of security requirements and penalties across the Member States;
- the high incident notification thresholds; and
- the highly fragmented supervisory framework.

Cooperation at EU level

The Cooperation Group was deemed effective across all three stakeholder groups in assisting Member States in building capacity and exchanging best practices and experiences.

Similarly, the CSIRTs Network was overall deemed to have a positive impact in clarifying actors' role and responsibilities within the incident response process.

However, respondents frequently highlighted the need for improvements regarding communication and collaboration between the Cooperation Group and the CSIRTs Network.

Efficiency

Costs

The findings of the online surveys showed that the administrative and compliance costs brought about by the NIS Directive were deemed reasonable by most CAs, OESs and DSPs.

However, stakeholders taking part in the in-depth interviews frequently flagged the duplication of efforts in the implementation of the NIS Directive as having negative implications on costs, both in terms of human resources and time. Duplication was highlighted as a result of efforts undertaken to ensure compliance with multiple legislative texts, which often implies the existence of different reporting authorities, timelines, and thresholds.

Benefits

The NIS Directive was overall viewed as having contributed to the setting up of a horizontal framework for the security of networks and information systems at the EU level, triggering the implementation of security measures across the Member States and fostering collaboration and trust within the Union.

According to the results of the online surveys and the in-depth interviews, the main benefits of the NIS Directive were:

- increased trust in the digital economy,
- improved functioning of the internal market
- reduced impact of NIS incidents

Conclusions

Evidence from the targeted consultation activities reveal that the NIS Directive has relevance given society's ever greater dependency on ICT as well as the evolution of the cyber threat landscape. However, the results also reveal that Member States' capabilities are deemed uneven and sometimes insufficient to respond to cyber threats comprehensively and effectively, including cross-border incidents.

Stakeholders overall recognise that diffrent levels of preparedness within Member States persist, leading to fragmented approaches across the EU for ensuring a high level of cybersecurity.

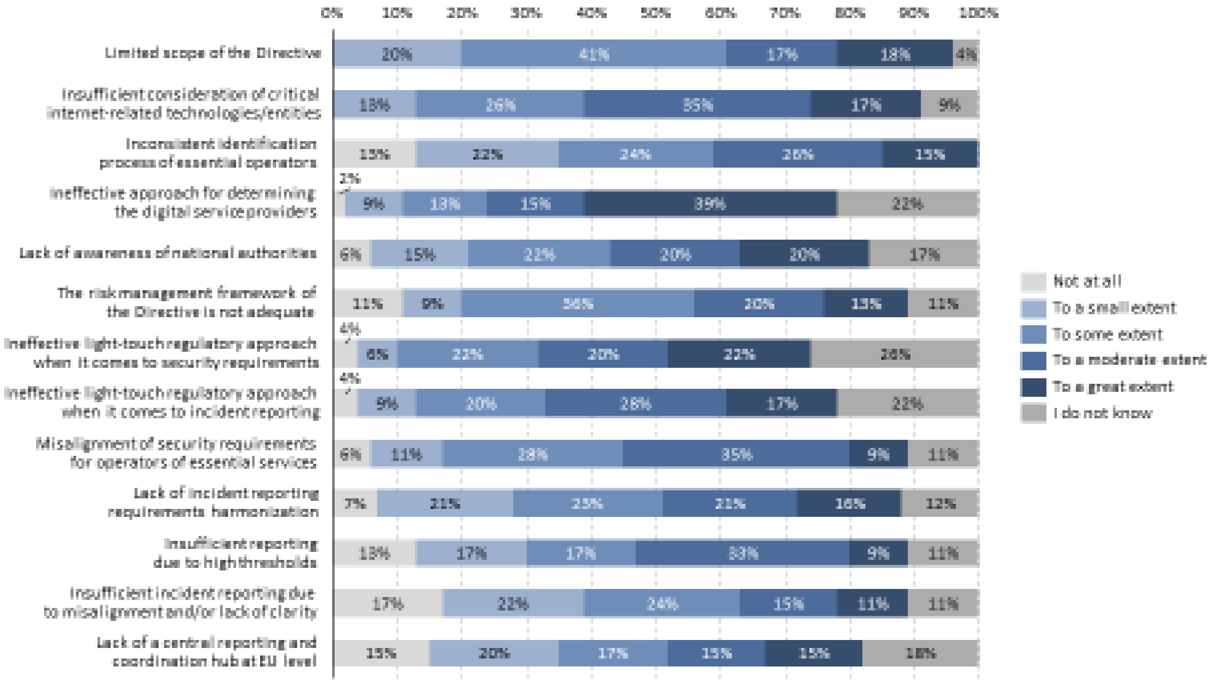
Based on the results of the targeted consultation, the points to consider in the review of the NIS Directive are as follows:

- lack of harmonisation across the Union when it comes to the identification of OESs
- insufficient consideration of critical internet-related technologies/entities, which may turn the entire digital ecosystem vulnerable
- legal concepts not fully defined, resulting in Members States interpreting them in their own laws which is potentially detrimental to the level-playing field.

Illustrative charts on extracts from the results of the survey targeting competent authorities

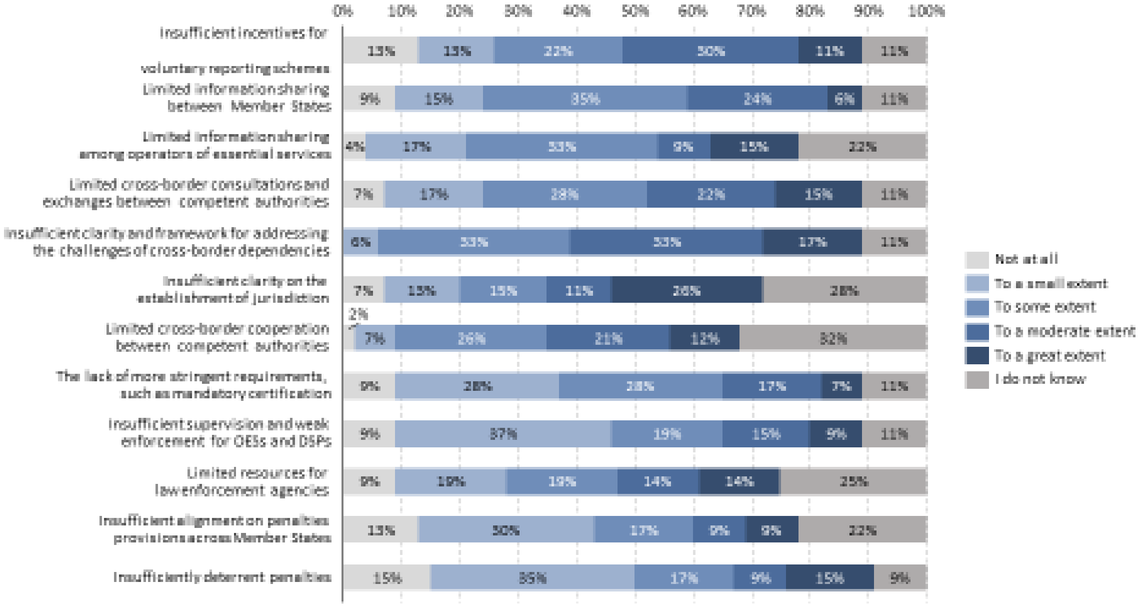
On the shortcomings of the NIS Directive

Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (1/2)



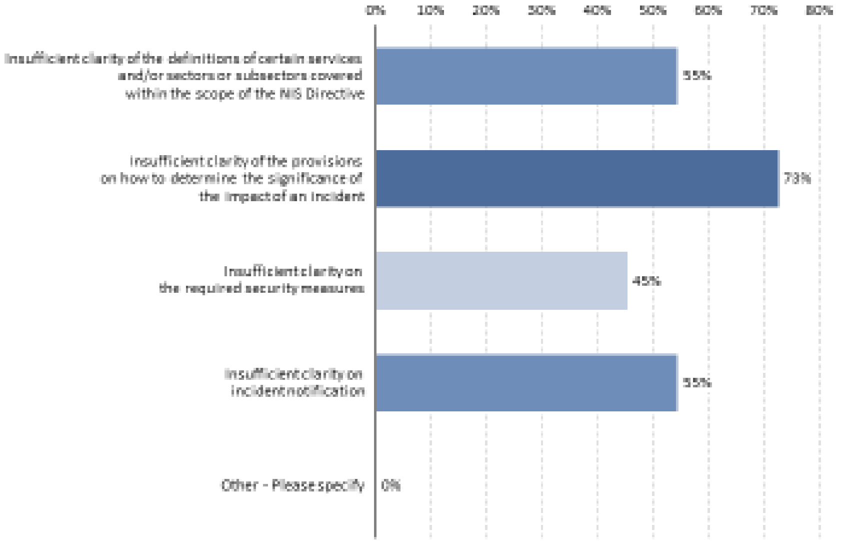
Source: Targeted online survey conducted by Wavestone with CAs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (1/2). N for CAs= 46

Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/2)



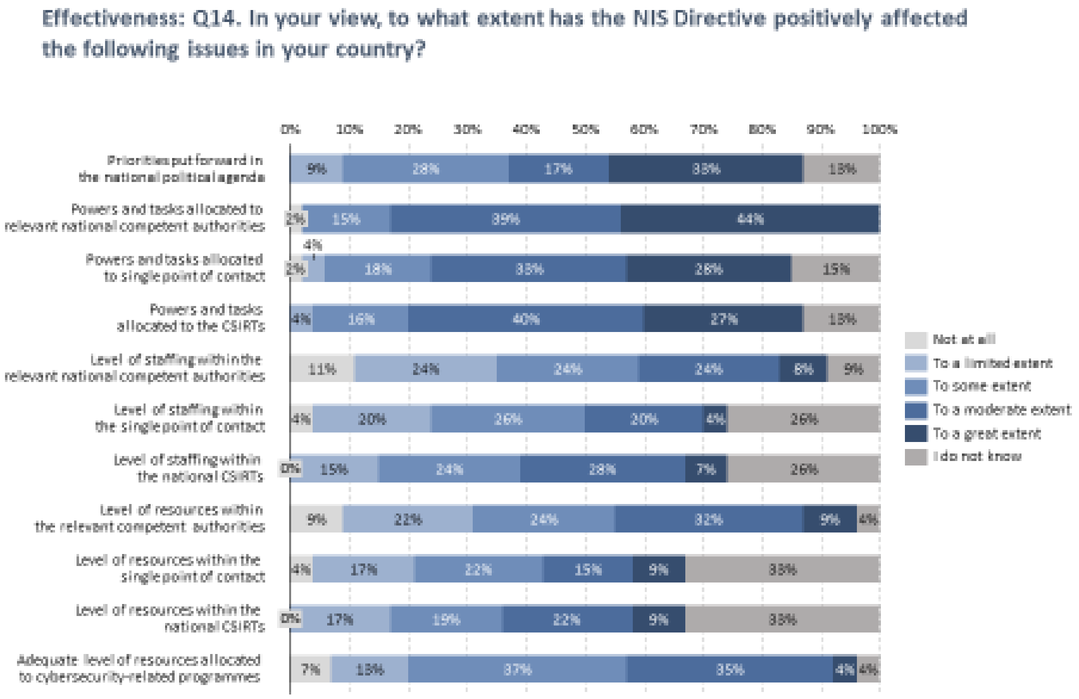
Source: Targeted online survey conducted by Wavestone with CAs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/2). N for CAs= 46

Coherence: Q10. What are the main problems that could impact the level of awareness of operators of essential services on their obligations?



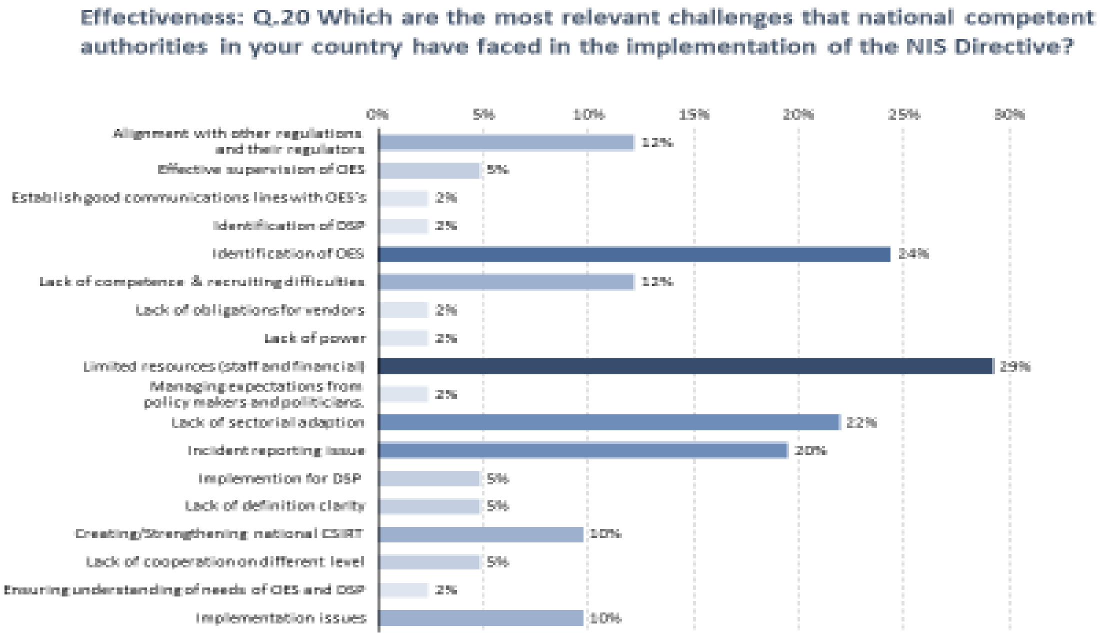
Source: Targeted online survey conducted by Wavestone with CAs. Q10. What are the main problems that could impact the level of awareness of operators of essential services on their obligations? N for CAs= 11

On the positive impact of the NIS Directive


Effectiveness: Q14. In your view, to what extent has the NIS Directive positively affected the following issues in your country?

Source: Targeted online survey conducted by Wavestone with CAs. Q14. In your view, to what extent has the NIS Directive positively affected the following issues in your country? N for CAs= 46

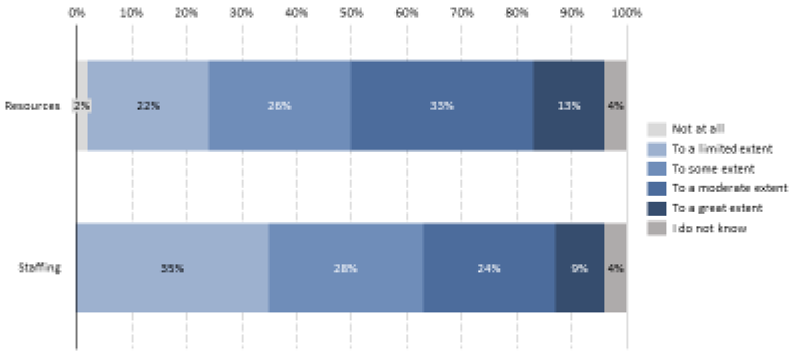
On challenges faced in the implementation of the NIS Directive


Effectiveness: Q.20 Which are the most relevant challenges that national competent authorities in your country have faced in the implementation of the NIS Directive?

Source: Targeted online survey conducted by Wavestone with CAs. Q.20 Which are the most relevant challenges that national competent authorities in your country have faced in the implementation of the NIS Directive? N for CAs= 41

On available resources

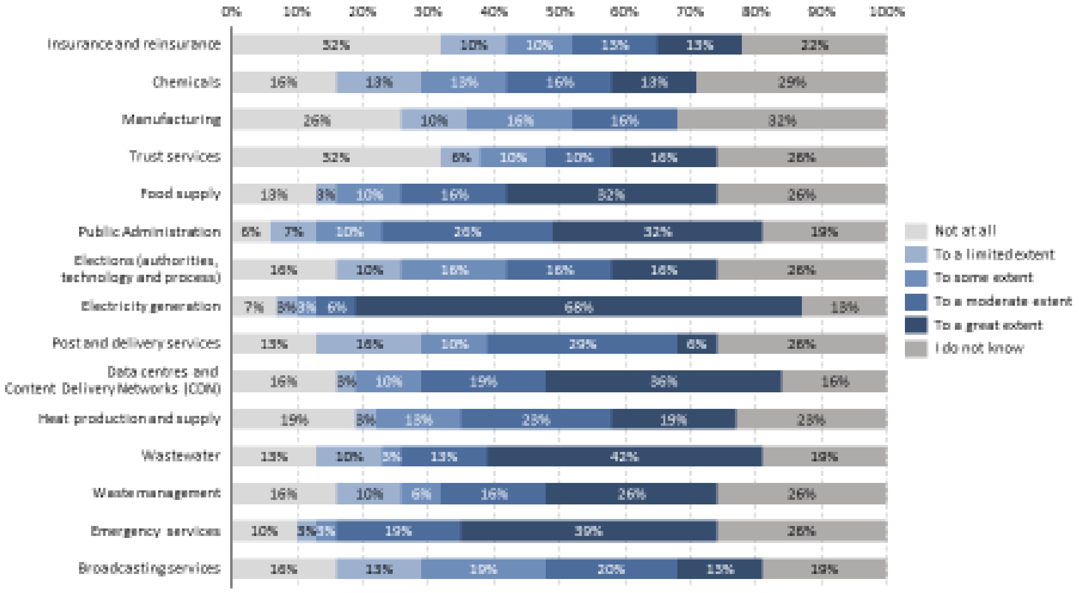
Effectiveness: Q21. Based on your experience, to what extent do national competent authorities dealing with the protection of network and information systems have adequate resources and staffing to fulfil their tasks efficiently?



Source: Targeted online survey conducted by Wavestone with CAs. Q21. Based on your experience, to what extent do national competent authorities dealing with the protection of network and information systems have adequate resources and staffing to fulfil their tasks efficiently? N for CAs= 46

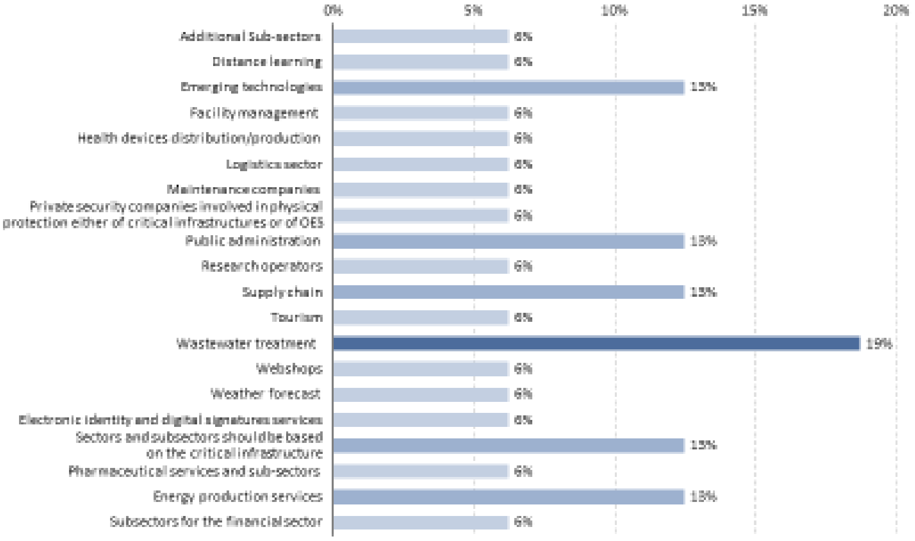
On the scope of the NIS Directive

Effectiveness: [Conditional Question: if "No" in Q44] Q45. In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile?



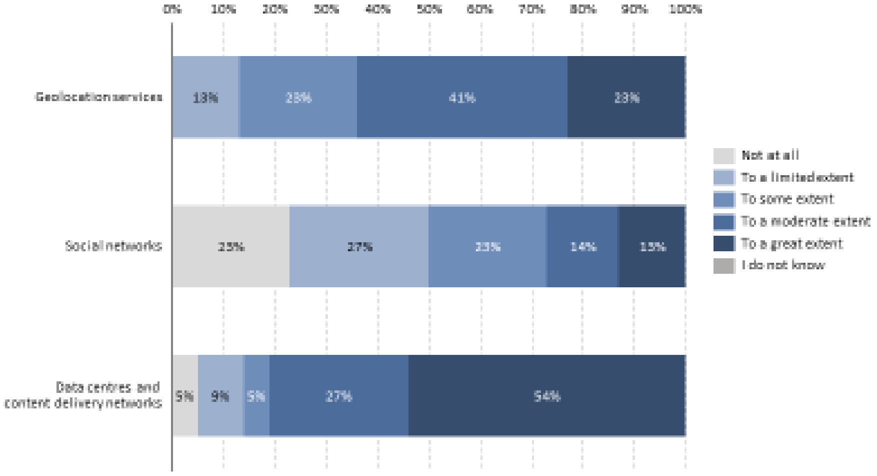
Source: Targeted online survey conducted by Wavestone with CAs. Q45. In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile? N for CAs= 31

Effectiveness: [Conditional Question: if "Yes" in Q46] Q48. Based on your answers to the previous questions, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole?



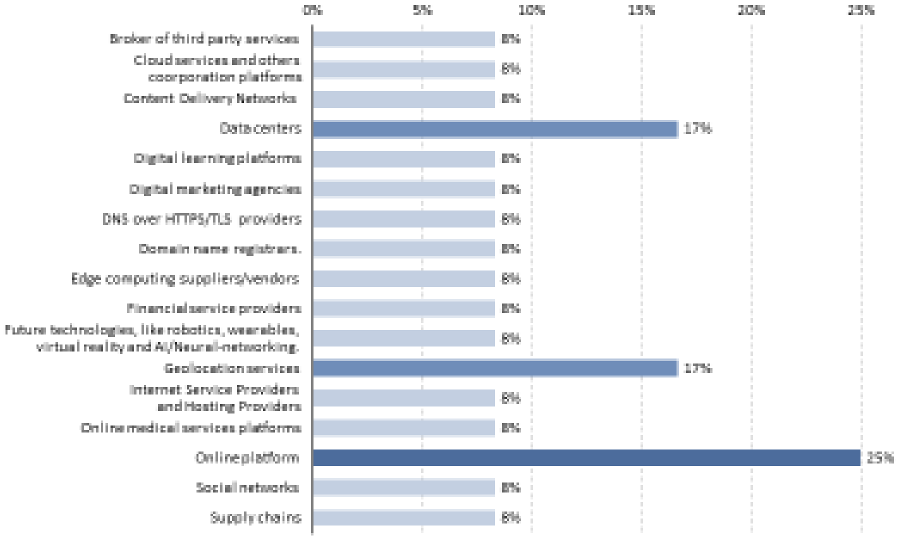
Source: Targeted online survey conducted by Wavestone with CAs. Q48. Based on your answers to the previous questions, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole? N for CAs= 16

Effectiveness: Conditional Question: if "No" in Q55] Q56. In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity-related risk profile?



Source: Targeted online survey conducted by Wavestone with Cas Q56. In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity-related risk profile? N for CAs= 22

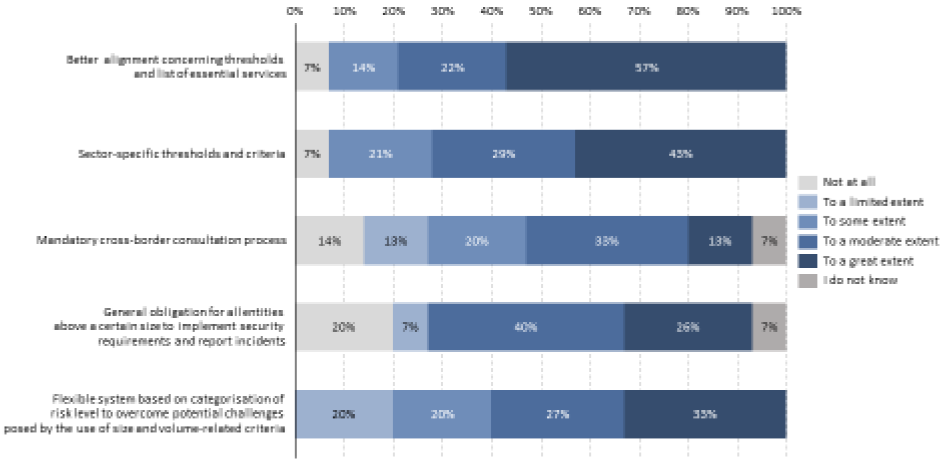
Effectiveness: [Conditional Question: if "No" in Q55] Q57. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union economy and society?



Source: Targeted online survey conducted by Wavestone with CAs. Q57. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union economy and society? N for CAs= 12

On identification of OES

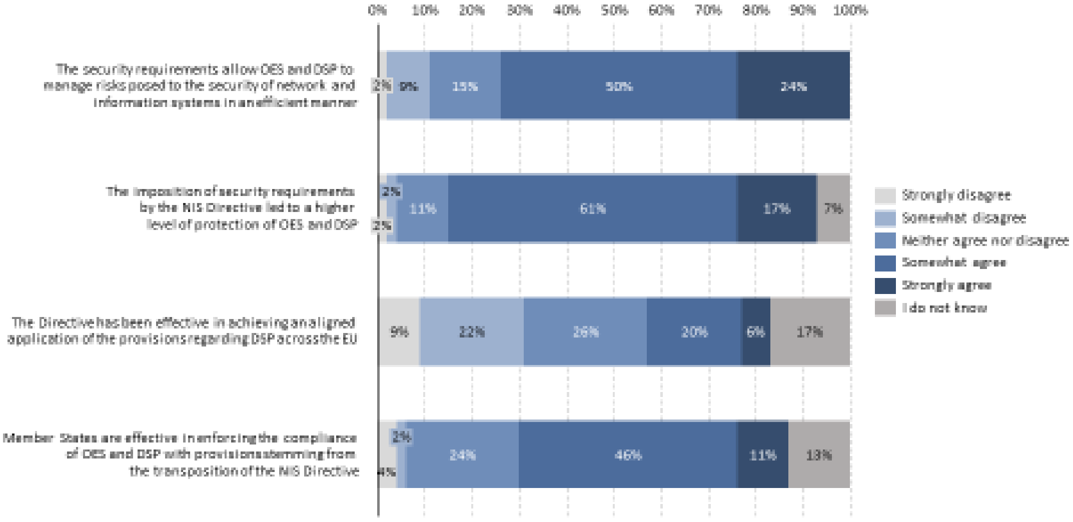
Effectiveness: [Conditional Question: if "Yes" in Q50] Q51. In your opinion, to what extent could the following aspects improve such identification system?



Source: Targeted online survey conducted by Wavestone with CAs. Q51. In your opinion, to what extent could the following aspects improve such identification system? N for CAs= 15

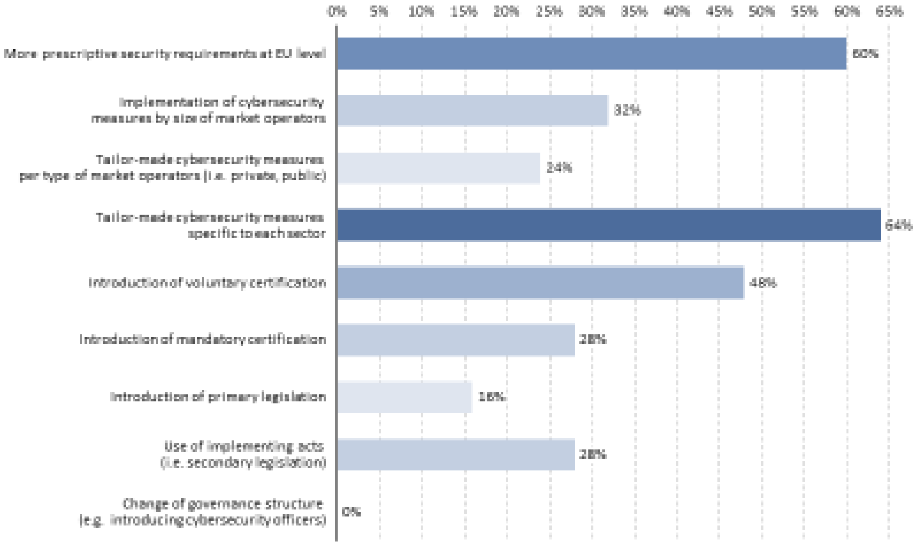
On security requirements and incident notifications

Effectiveness: Q59. Thinking about the security requirements and the incident notification provisions laid down in Article 14 and 16 of the Directive, and according your experience, to what extent would you agree with the following statements?



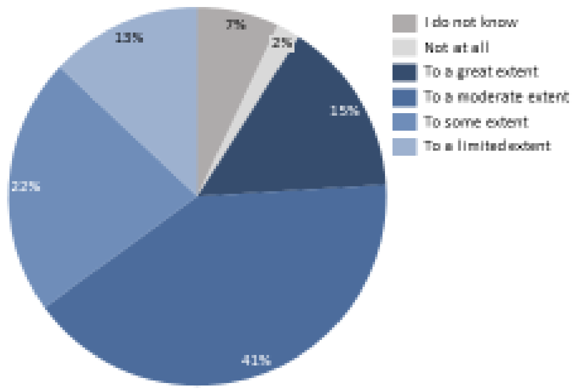
Source: Targeted online survey conducted by Wavestone with CAs. Q59. Thinking about the security requirements and the incident notification provisions laid down in Article 14 and 16 of the Directive, and according your experience, to what extent would you agree with the following statements? N for CAs= 46

Effectiveness: [Conditional Question: if "To a moderate extent", "To a great extent" in Q62] Q63. Which of the below options should be considered as means to achieve further alignment of security requirements?



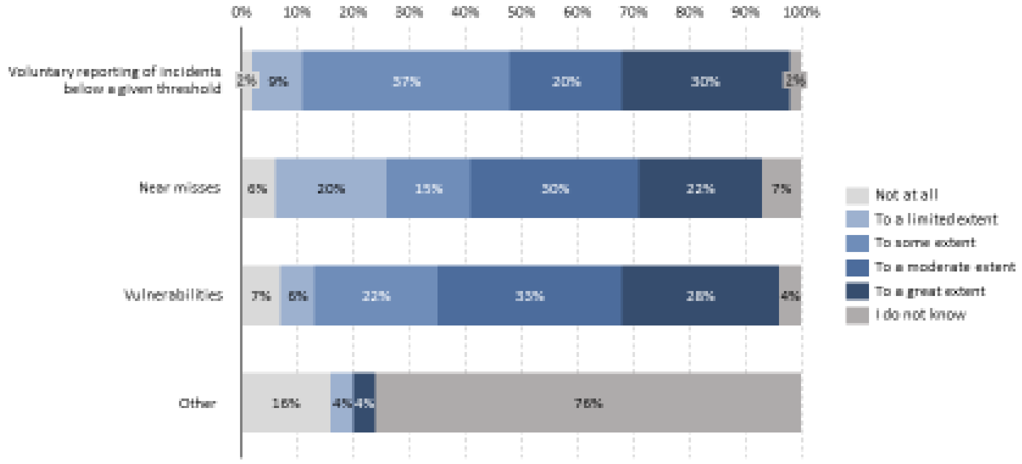
Source: Targeted online survey conducted by Wavestone with CAs. Q63. Which of the below options should be considered as means to achieve further alignment of security requirements? N for CAs= 25

Effectiveness: Q68. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension?



Source: Targeted online survey conducted by Wavestone with CAs. Q68. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension? N for CAs= 46

Effectiveness: Q70. In your opinion, to what extent do you consider those new ways of reporting relevant incidents should be explored such as voluntary reporting schemes, inclusion of additional types of cybersecurity-related incidents such as near misses or vulnerabilities?



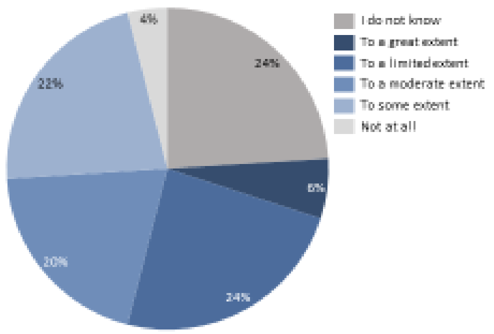
Other:

- Voluntary reporting already exists.
- NL is in favor of looking into qualitative notification requirements that can indicate (the probability of) an incident in an early phase.

Source: Targeted online survey conducted by Wavestone with CAs. Q70. In your opinion, to what extent do you consider those new ways of reporting relevant incidents should be explored such as voluntary reporting schemes, inclusion of additional types of cybersecurity-related incidents such as near misses or vulnerabilities? N for CAs= 46

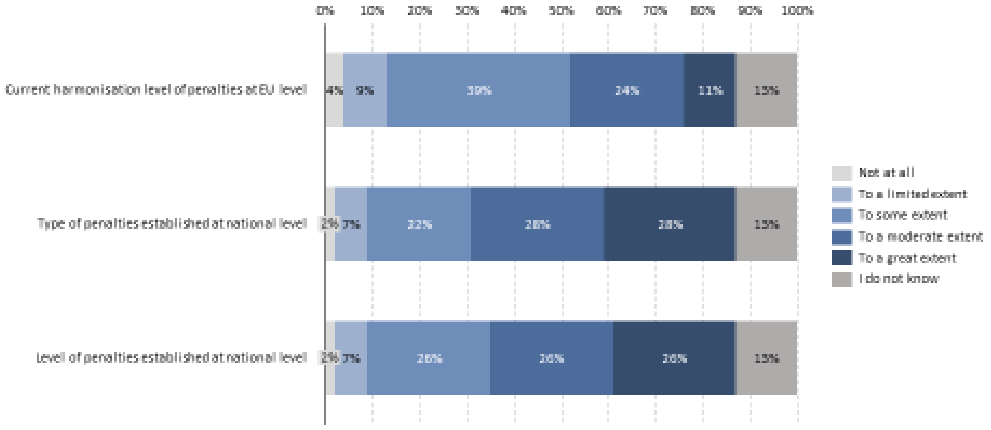
On supervision and enforcement

Effectiveness: Q75. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital services providers effective?



Source: Targeted online survey conducted by Wavestone with CAs. Q75. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital services providers effective? N for CAs= 46

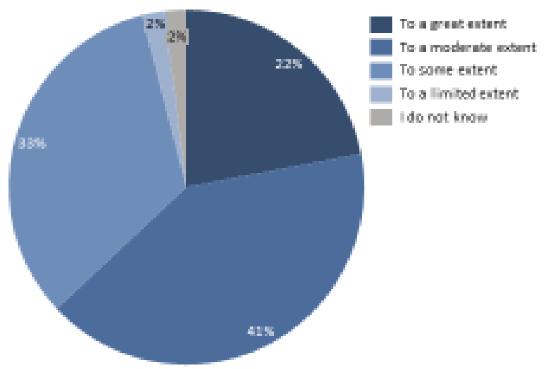
Effectiveness: Q76. Thinking about penalties both at EU and national level, to what extent do you consider the following measures effective?



Source: Targeted online survey conducted by Wavestone with CAs. Q76. Thinking about penalties both at EU and national level, to what extent do you consider the following measures effective? N for CAs= 46

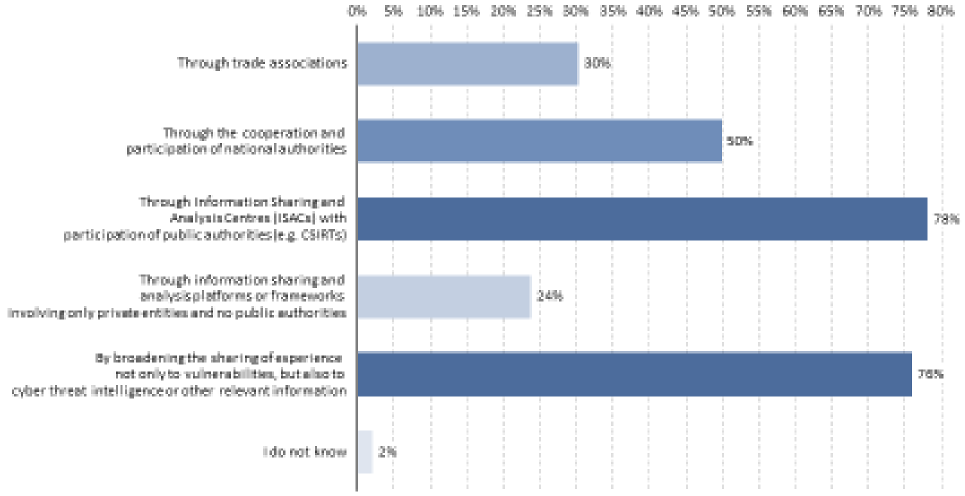
On information sharing and cooperation

Effectiveness: Q83. In your view, to what extent do you think the level of information sharing between the public and the private sectors is effective?



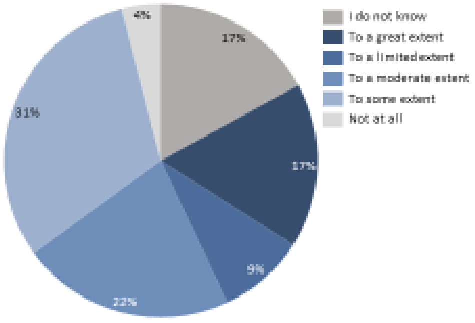
Source: Targeted online survey conducted by Wavestone with CAs. Q83. In your view, to what extent do you think the level of information sharing between the public and the private sectors is effective? N for CAs= 46

Effectiveness: Q85. In your view, how could a better information sharing framework between companies be promoted?



Source: Targeted online survey conducted by Wavestone with CAs. Q85. In your view, how could a better information sharing framework between companies be promoted? N for CAs= 46

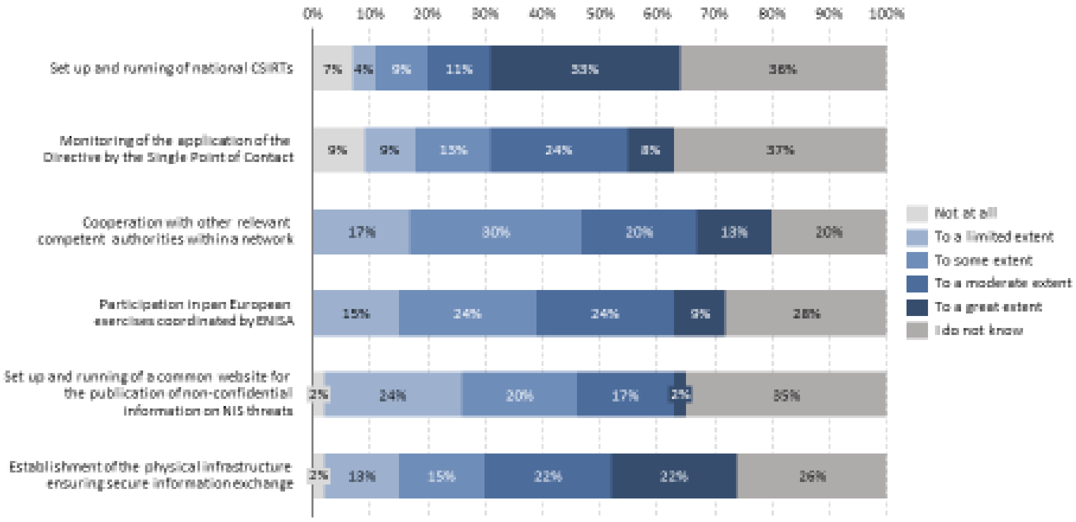
Effectiveness: Q86. In your opinion, and taking into account the ongoing policy initiatives on cybersecurity crises response (notably the implementation of the Blueprint Recommendation), to what extent a harmonisation at EU level of the national crisis management measures would help ensure a more effective coordinated EU response to large-scale incidents and crises?



Source: Targeted online survey conducted by Wavestone with CAs. Q86. In your opinion, and taking into account the ongoing policy initiatives on cybersecurity crises response (notably the implementation of the Blueprint Recommendation), to what extent a harmonisation at EU level of the national crisis management measures would help ensure a more effective coordinated EU response to large-scale incidents and crises? N for CAs= 46

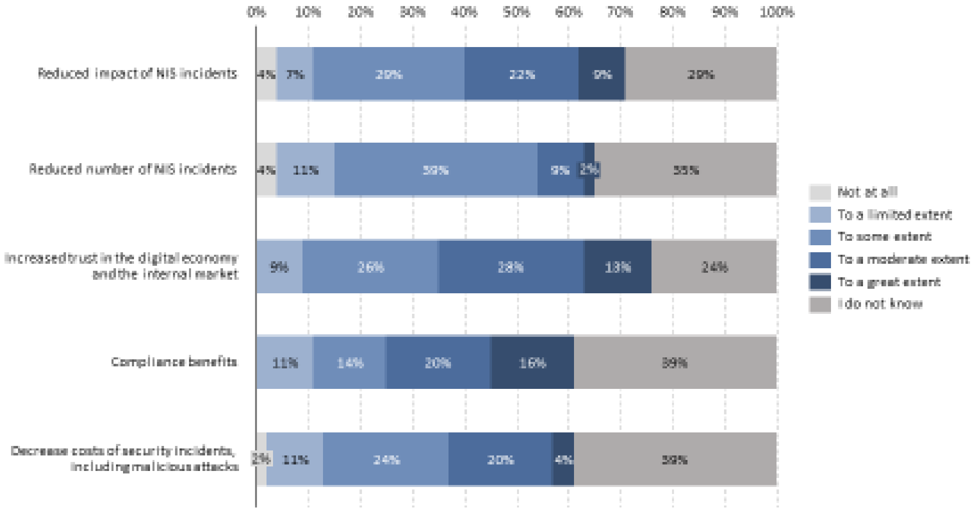
On efficiency, compliance costs and benefits

Efficiency: Q87. Considering the following compliance costs with the provisions of the NIS Directive, to what extent are they significant for the competent authorities in your country?



Source: Targeted online survey conducted by Wavestone with CAs. Q87. Considering the following compliance costs with the provisions of the NIS Directive, to what extent are they significant for the competent authorities in your country? N for CAs= 46

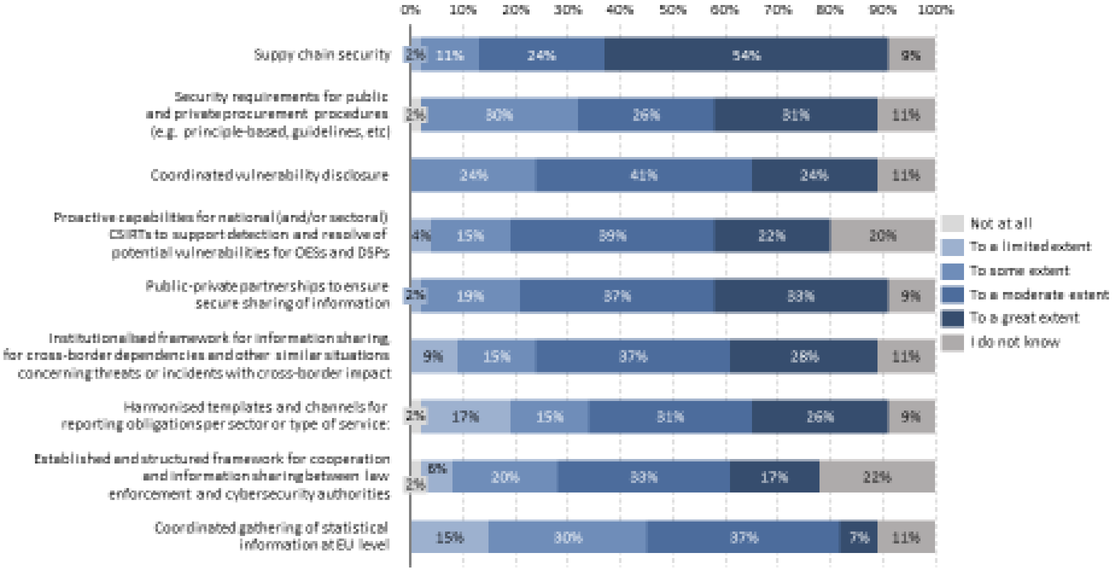
Efficiency: Q96. Based on your experience, to what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your Case?



Source: Targeted online survey conducted by Wavestone with CAs. Q96. Based on your experience, to what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your Case? N for CAs= 46

On EU added value of new policy concepts

EU added value: Q102. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered?

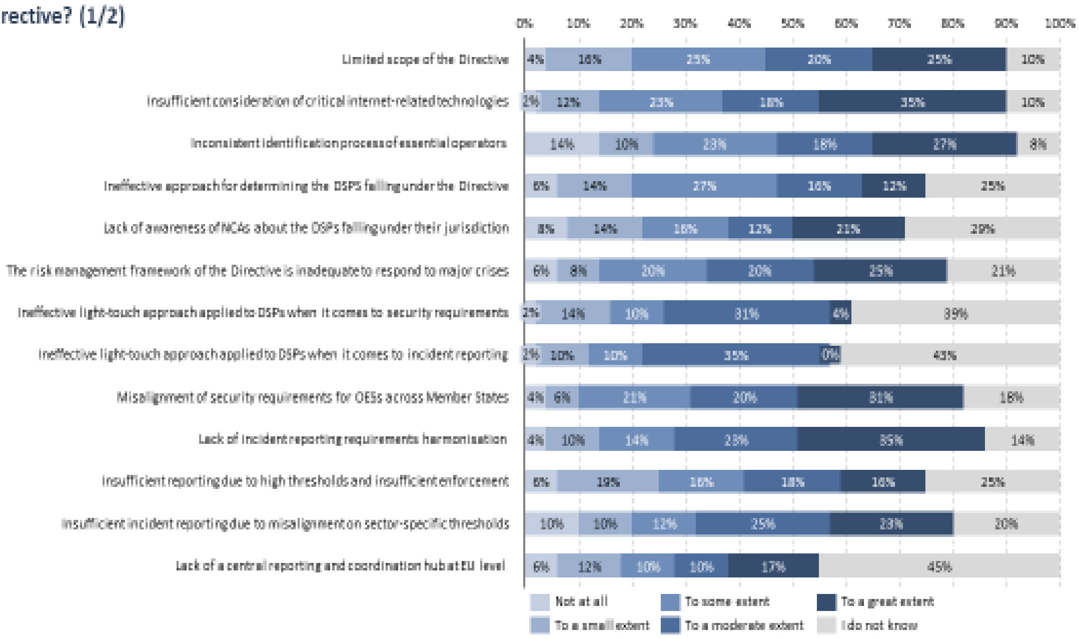


Source: Targeted online survey conducted by Wavestone with CAs. Q102. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? N for CAs= 46

<u>Illustrative charts on extracts from the results of the survey targeting operators of essential services</u>

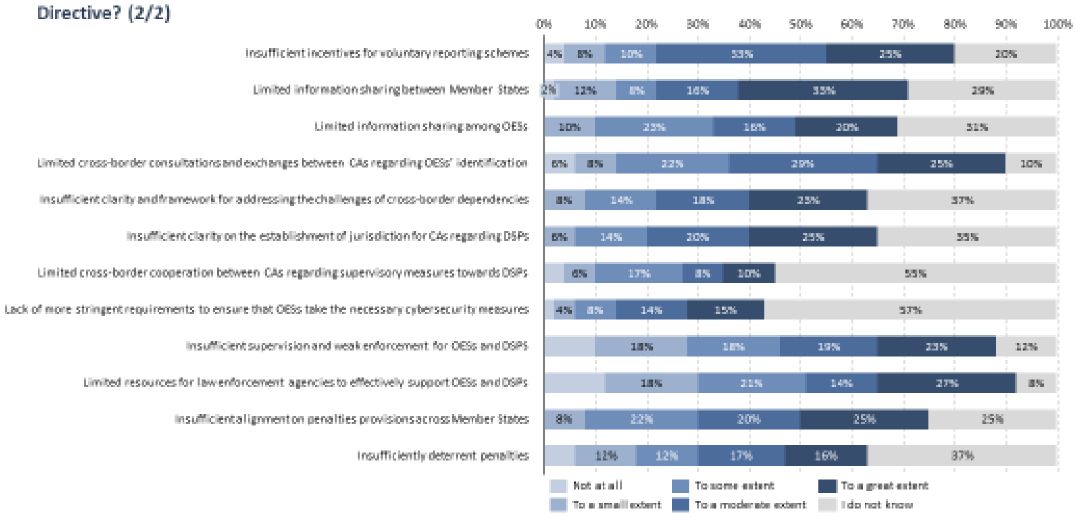
On the shortcomings of the NIS Directive

Relevance: Q3.Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (1/2)



<u>Source</u>: Targeted online survey conducted by Wavestone with OESs. Q3.Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for OESs=49

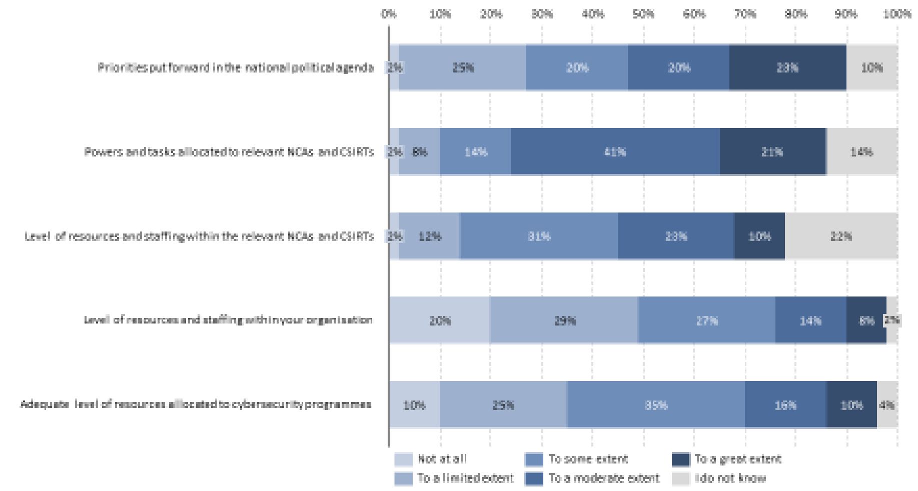
Relevance: Q3.Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/2)



<u>Source</u>: Targeted online survey conducted by Wavestone with OESs. Q3.Taking account of the current realities and potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for OESs=49

On the positive effects of the NIS Directive

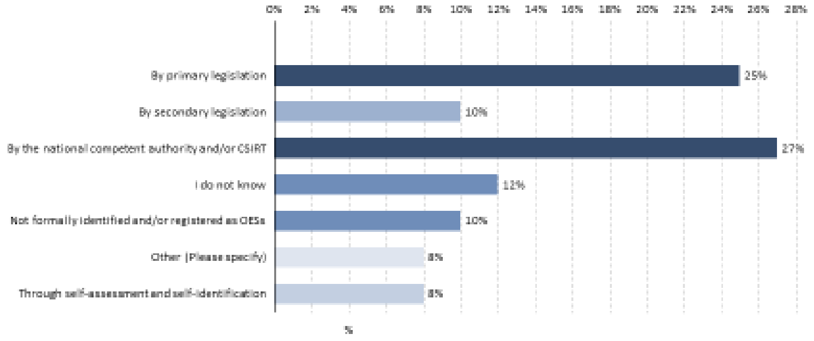
Effectiveness: Q13.To what extent has the NIS Directive positively affected the following issues in your country?



Source: Targeted online survey conducted by Wavestone with OESs. Q13.To what extent has the NIS Directive positively affected the following issues in your country? N for OESs=49

On identification of OES

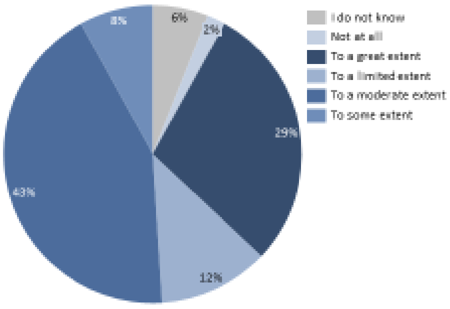
Effectiveness: Q16.How were you identified as an operator of essential services in your respective Member State?



Other	In Italy and Spain by CAs
	Primary or secondary legislation
	In Romania by self-identification

Source: Targeted online survey conducted by Wavestone with OESs. Q16.How were you identified as an operator of essential services in your respective Member State? N for OESs=49

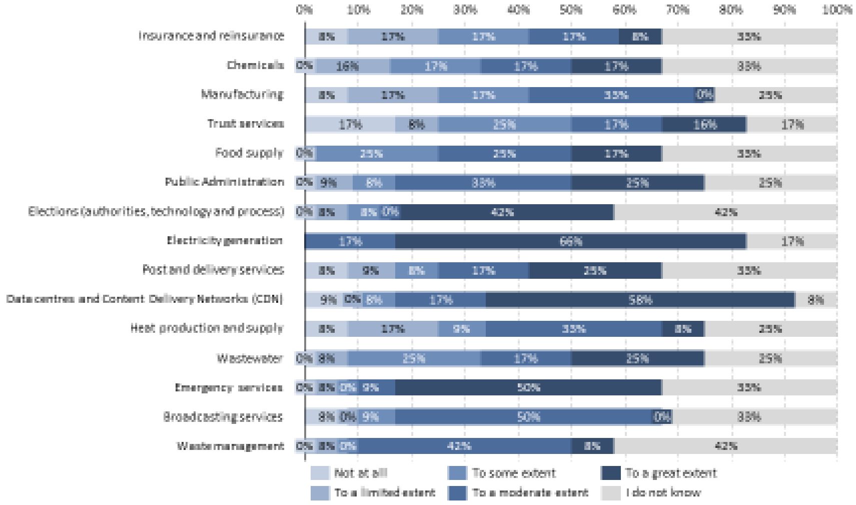
Effectiveness: Q18.In your opinion, to what extent are the above-mentioned criteria for the identification of operators of essential services comprehensive and/or relevant for the purpose of determining the scope of the NIS Directive?



Source: Targeted online survey conducted by Wavestone with OESs. Q18.In your opinion, to what extent are the above-mentioned criteria for the identification of operators of essential services comprehensive and/or relevant for the purpose of determining the scope of the NIS Directive? N for OESs=49

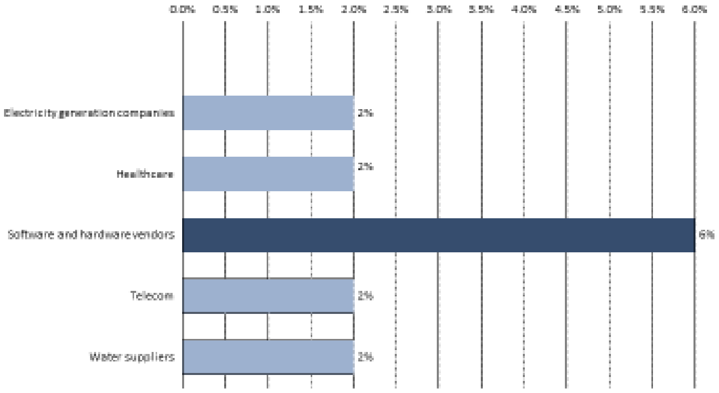
On the scope of the NIS Directive

Effectiveness: Q23. In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile? Please tick the most appropriate answer that applies for each statement.



Source: Targeted online survey conducted by Wavestone with OESs. Q23. In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile? Please tick the most appropriate answer that applies for each statement. N for OESs=12

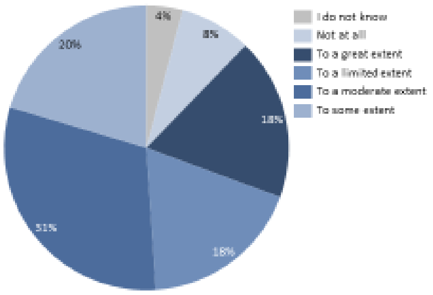
Effectiveness: Q24.Based on your answer to the previous question, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole? Please elaborate.



Source: Targeted online survey conducted by Wavestone with DESs. Q24.Based on your answer to the previous question, do you think there are additional sectors and sub-sectors currently not in the scope of the Directive that should be part of Annex II when it comes to the provision of services essential for the economy and society as a whole? Please elaborate. N for DESs=12

On resources

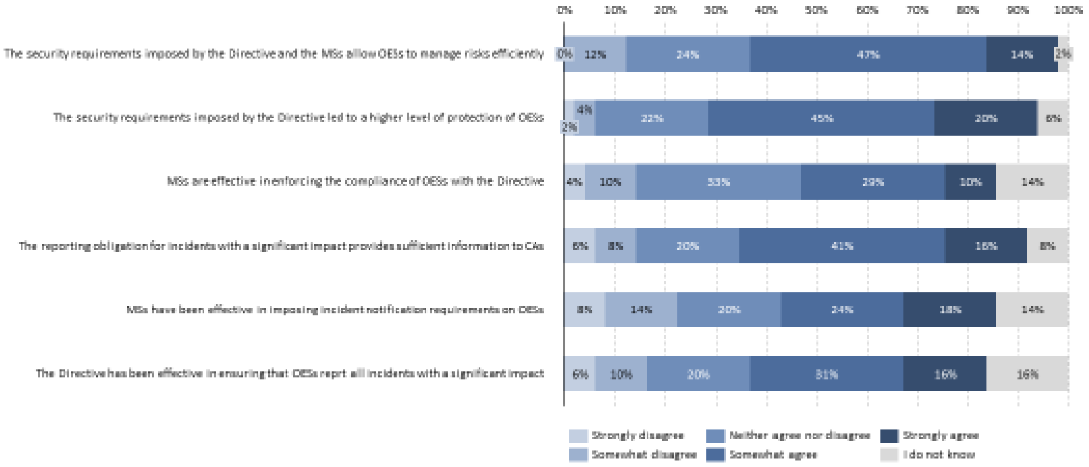
Effectiveness: Q30.Based on your experience, to what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate?



Source: Targeted online survey conducted by Wavestone with DESs. Q30.Based on your experience, to what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate? N for DESs=49

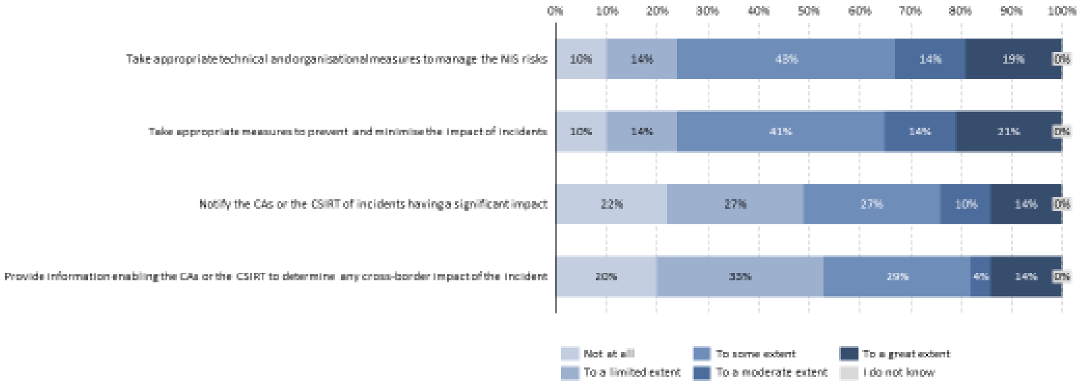
On security requirements and incident notifications

Effectiveness: Q32.To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 14 of the Directive?



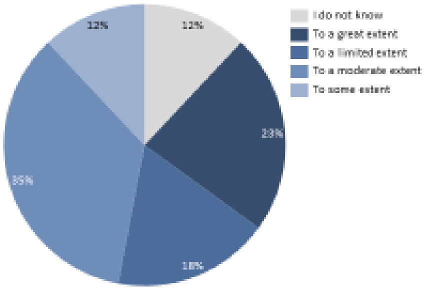
Source: Targeted online survey conducted by Wavestone with OESs. Q32.To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 14 of the Directive? N for OESs=49

Effectiveness: Q33. Considering the technical and organisational requirements put forward in Article 14 of the NIS Directive to manage the risks posed to the operators of essential services' security of network and information systems used in the context of offering services referred to in Annex II within the Union, to what extent did you face challenges in the implementation of the following requirements? Considering the requirements of operators of essential services listed below, please tick the most appropriate statement.



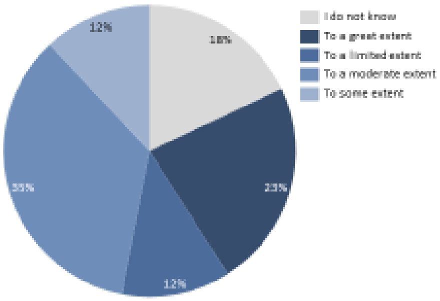
Source: Targeted online survey conducted by Wavestone with OESs. Q33. Considering the technical and organisational requirements put forward in Article 14 of the NIS Directive to manage the risks posed to the operators of essential services' security of network and information systems used in the context of offering services referred to in Annex II within the Union, to what extent did you face challenges in the implementation of the following requirements? Considering the requirements of operators of essential services listed below, please tick the most appropriate statement. N for OESs=49

Effectiveness: Q35.To what extent do the requirements for security measures differ from one Member State to the other? Please reply taking account of your direct experience.



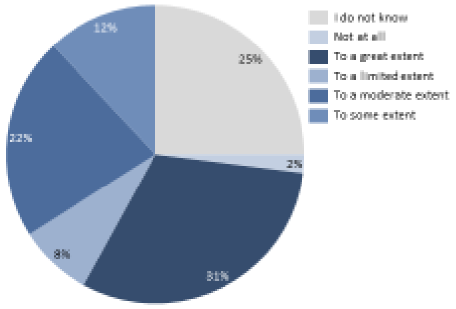
Source: Targeted online survey conducted by Wavestone with OESs. Q35.To what extent do the requirements for security measures differ from one Member State to the other? Please reply taking account of your direct experience. N for OESs=49

Effectiveness: Q37.In your opinion, to what extent the incident notification obligations differ from one Member State to the other? Please reply taking account of your direct experience.



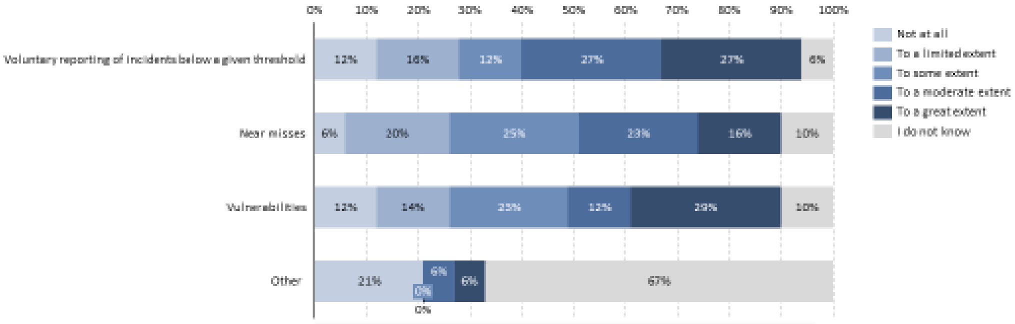
Source: Targeted online survey conducted by Wavestone with OESs. Q37.In your opinion, to what extent the incident notification obligations differ from one Member State to the other? Please reply taking account of your direct experience. N for OESs=49

Effectiveness: Q41. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension?



Source: Targeted online survey conducted by Wavestone with OESs. Q41. In your view, to what extent should the incident notifications requirements be better streamlined to allow for more relevant incidents to be reported, in particular for incidents with cross-border dimension? N for OESs=49

Effectiveness: Q43. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities? Considering new ways of reporting listed below, please tick the most appropriate answer.



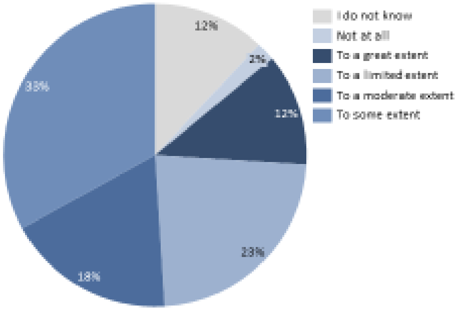
Other

Mediation
Use existing technologies (vulnerability scanners and ticketing systems)
Encourage participation in private sector initiatives
Not at all
Adopt whistleblowing concept
Use sector specific incentives and schemes
Share root causes, lessons learned, investigations

Source: Targeted online survey conducted by Wavestone with OESs. Q43. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities? Considering new ways of reporting listed below, please tick the most appropriate answer. N for OESs=49

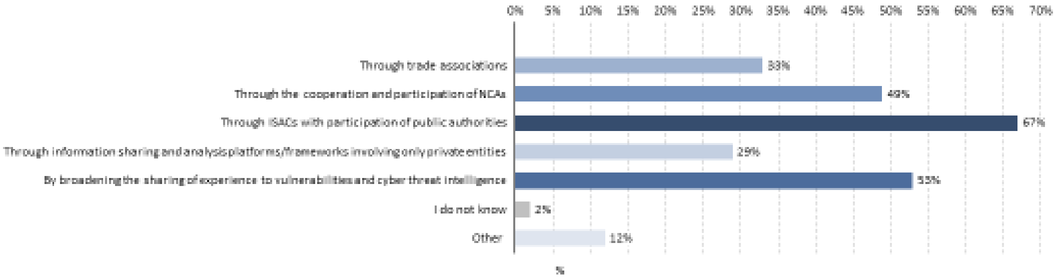
On information sharing and cooperation

Effectiveness: Q45. To what extent do you think the level of information sharing between public and the private sectors is effective?



Source: Targeted online survey conducted by Wavestone with DESs. Q45. To what extent do you think the level of information sharing between public and the private sectors is effective? N for DESs=49

Effectiveness: Q50. In your view, how could a better information sharing framework between companies be promoted? Please tick all that apply.

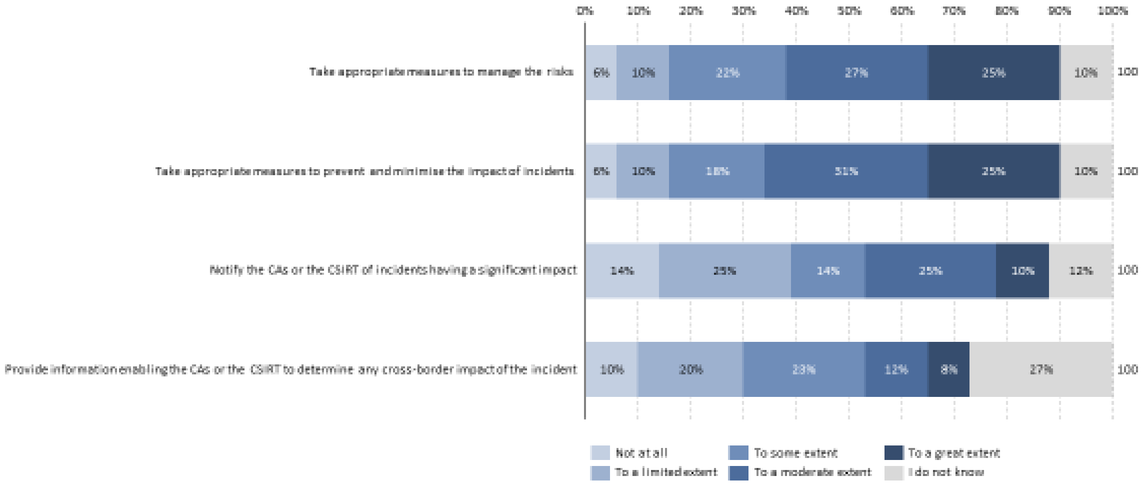


Other
- By providing supporting services (meetings, workshops, a platform)
- By the companies, internally
- Trust
- Through sectoral CERTs
- Through sectorial national ISACs
- Through a common and shared definition of the scope of data

Source: Targeted online survey conducted by Wavestone with DESs. Q50. In your view, how could a better information sharing framework between companies be promoted? Please tick all that apply. N for DESs=49

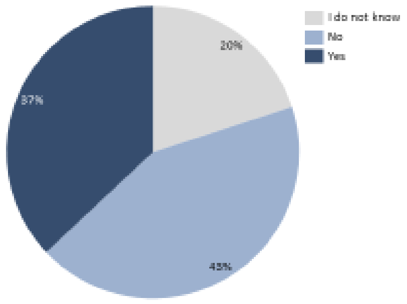
On efficiency, compliance costs and benefits

Efficiency: Q51.Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 14, to what extent were they significant for your organisation?



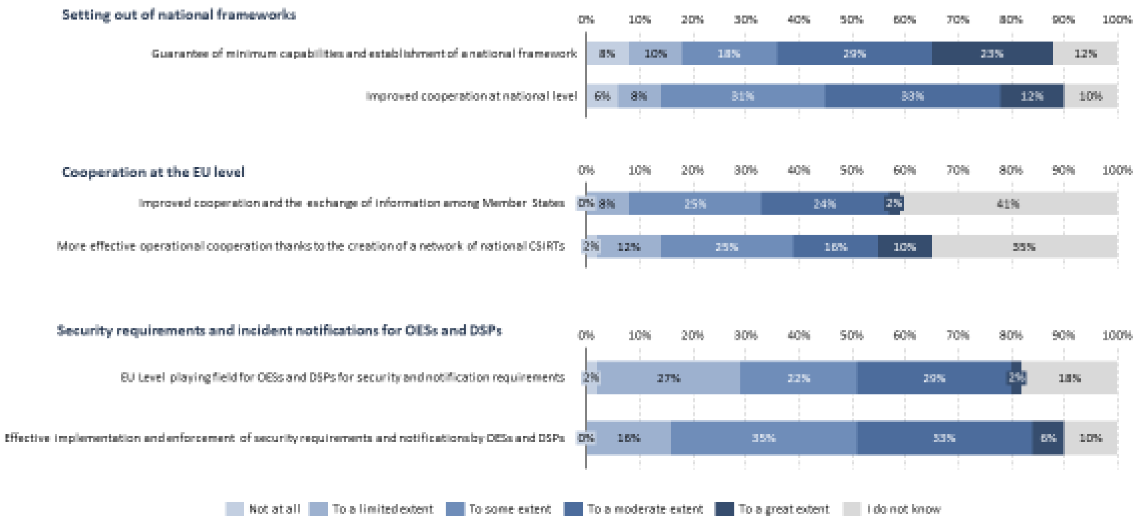
Source: Targeted online survey conducted by Wavestone with DESs. Q51.Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 14, to what extent were they significant for your organisation? N for DESs=49

Efficiency: Q52. Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement?



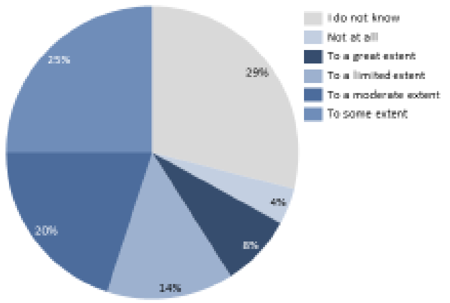
Source: Targeted online survey conducted by Wavestone with DESs. Q52. Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement? N for DESs=49

Efficiency: Q57. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case?



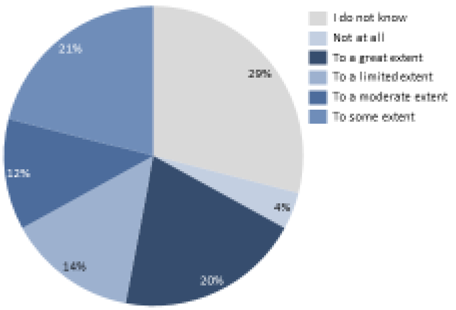
Source: Targeted online survey conducted by Wavestone with OESs. Q57. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case? N for OESs=49

Effectiveness: Q59. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought?



Source: Targeted online survey conducted by Wavestone with OESs. Q59. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought? N for OESs=49

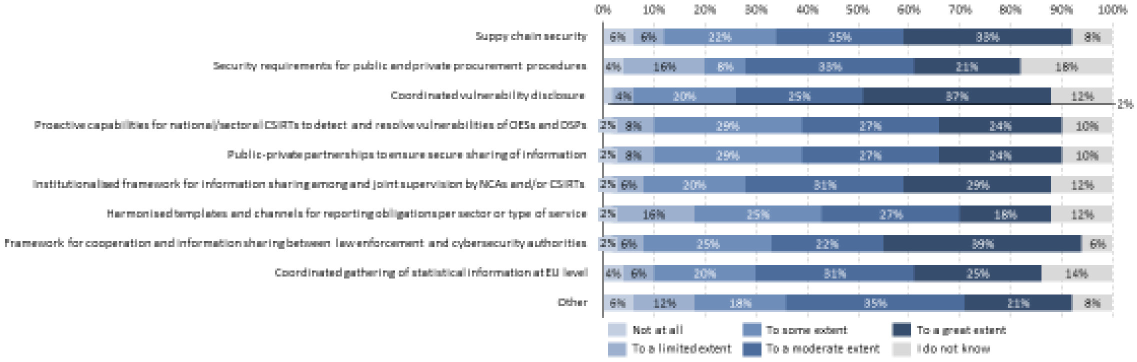
Effectiveness: Q62.To what extent do you think that different reporting thresholds and deadlines across the EU create unnecessary administrative burden for operators of essential services (e.g. when operating in different countries)?



Source: Targeted online survey conducted by Wavestone with OESs. Q62.To what extent do you think that different reporting thresholds and deadlines across the EU create unnecessary administrative burden for operators of essential services (e.g. when operating in different countries)? N for OESs=49

On new policy concepts

Effectiveness: Q64.In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? Considering the new policy measures listed below, please tick the most appropriate answer.



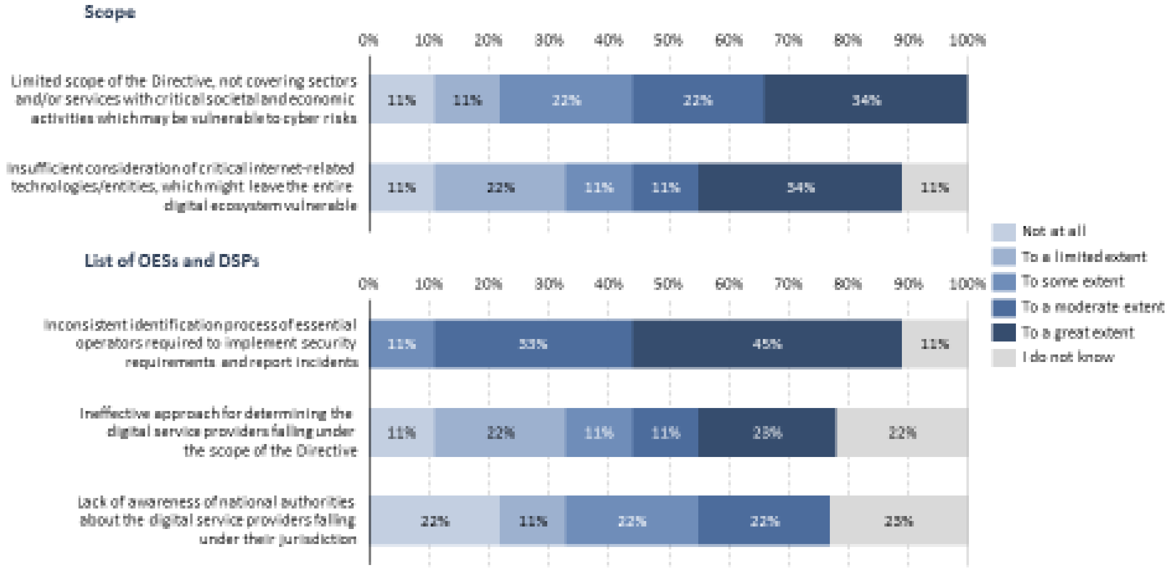
Other	Enhance segregation of duties within OES/DSP Creating a common and compulsory framework encompassing a risk analysis methodology Enhance the role of Security Managers Explore the links among existing actors and the possibility to harmonise incident handling Improved sharing with cross-border private sector initiatives (existing ISACs) Obligation of manufacturers to report critical weaknesses Two-way sharing Providers of software and hardware should be regulated

Source: Targeted online survey conducted by Wavestone with OESs. Q64.In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? Considering the new policy measures listed below, please tick the most appropriate answer. N for OESs=49c

<u>Illustrative charts on extracts from the results of the survey targeting digital service providers</u>

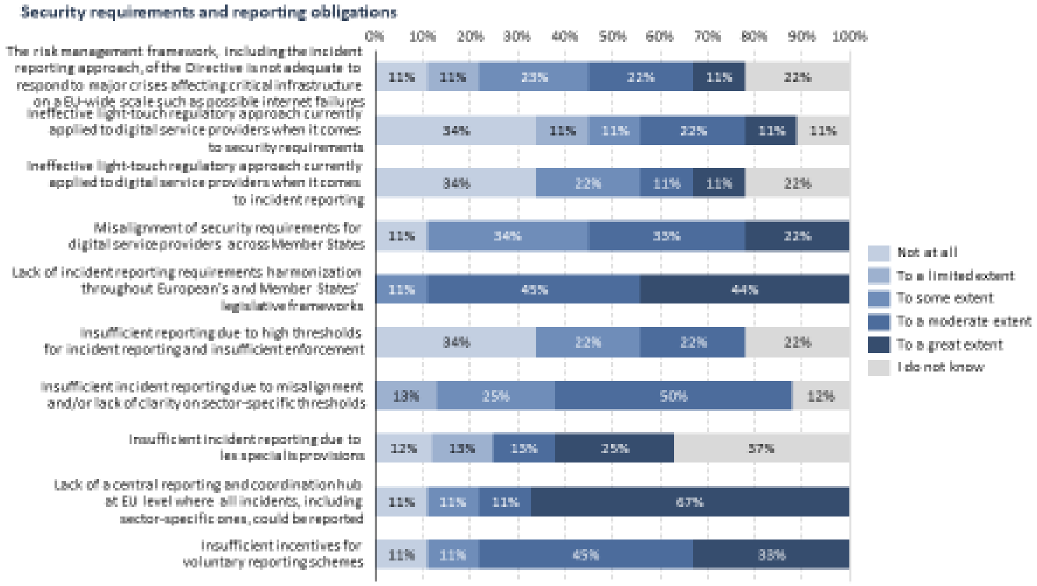
On shortcomings of the NIS Directive

Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (1/4)



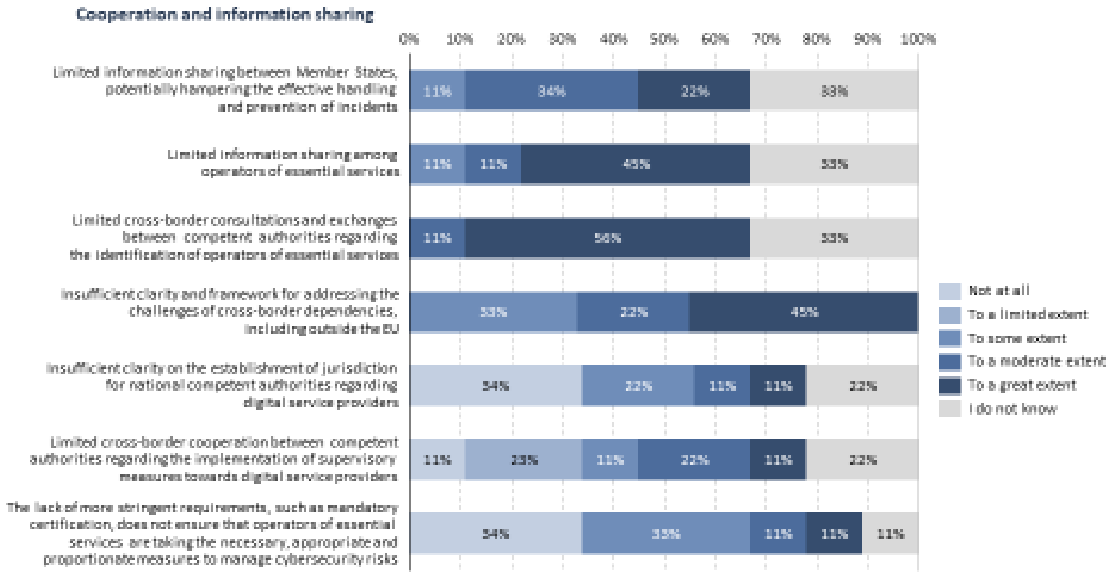
<u>Source</u>: Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive?N for DSPs= 9

Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (2/4)



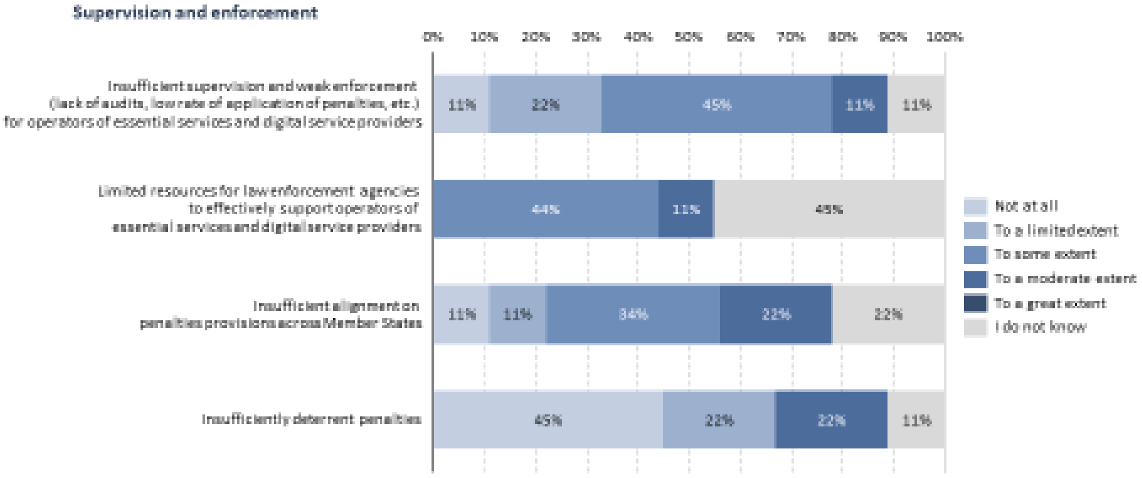
Source: Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for DSPs= 9

Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (3/4)



Source: Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for DSPs= 9

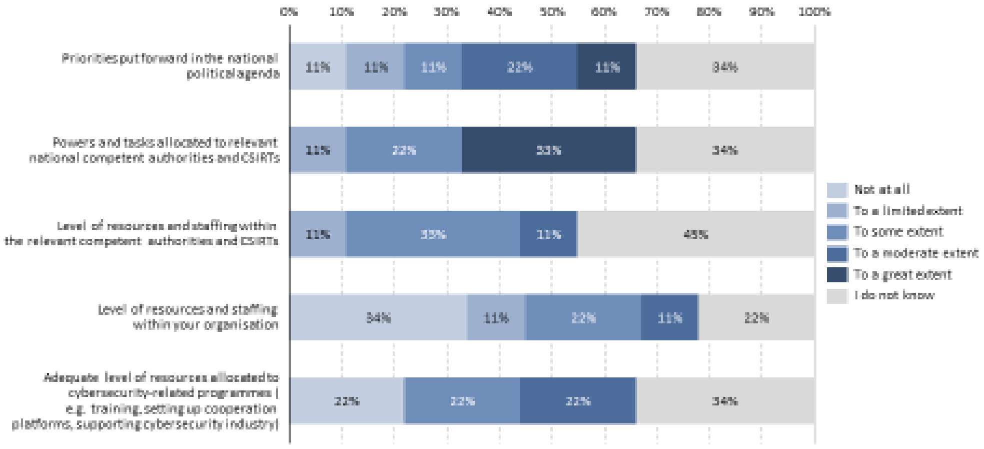
Relevance: Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? (4/4)



Source: Targeted online survey conducted by Wavestone with DSPs. Q3. Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive? N for DSPs= 9

On the positive effects of the NIS Directive

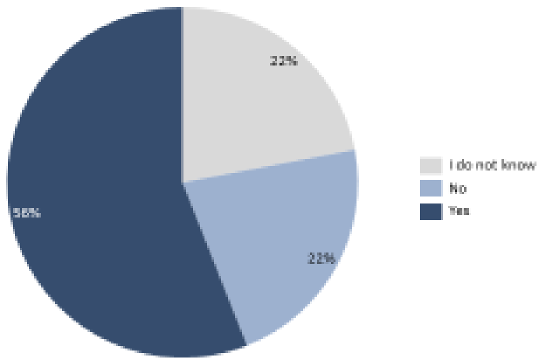
Effectiveness: Q13. In your view, to what extent has the NIS Directive positively affected the following issues in your country?



Source: Targeted online survey conducted by Wavestone with DSPs. Q13. In your view, to what extent has the NIS Directive positively affected the following issues in your country? N for DSPs= 9

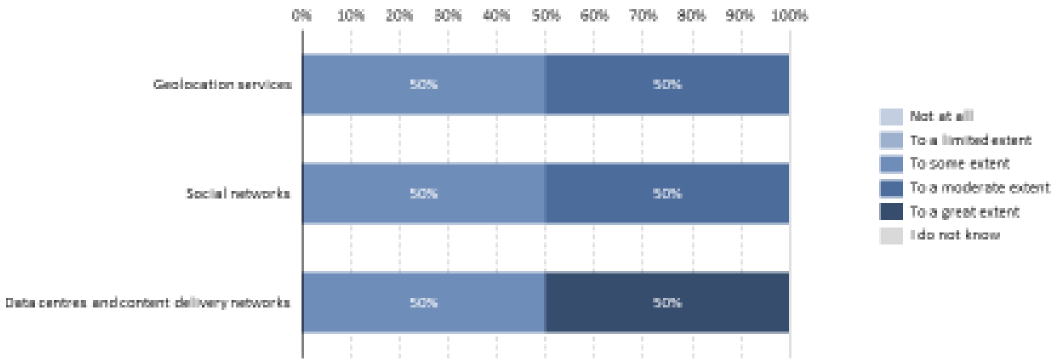
On the scope of the NIS Directive

Effectiveness: Q16. In your view, does Annex III of the NIS Directive effectively cover all types of digital service providers considered as essential for the functioning of the Union's economy and society?



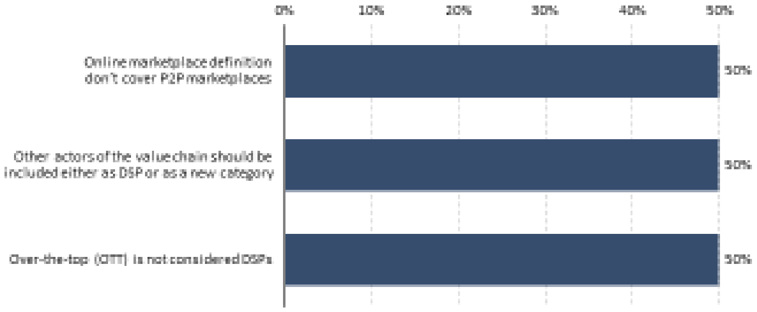
Source: Targeted online survey conducted by Wavestone with DSPs. Q16. In your view, does Annex III of the NIS Directive effectively cover all types of digital service providers considered as essential for the functioning of the Union's economy and society? N for DSPs= 9

Effectiveness: Conditional question [If "No" was answered in Q16] Q17. In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity related risk profile?



Source: Targeted online survey conducted by Wavestone with DSPs. Conditional question [If "No" was answered in Q16] Q17. In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity related risk profile? N for DSPs= 2

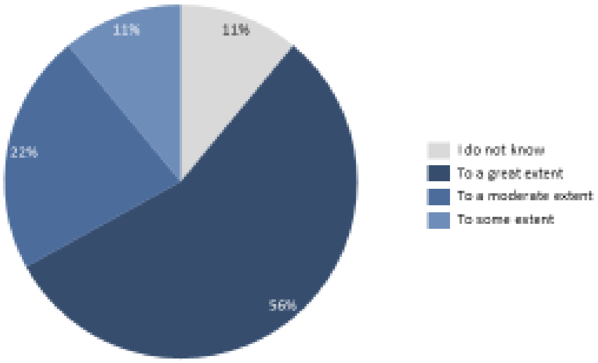
Effectiveness: Conditional question [If "No" was answered in Q16] Q18. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union's economy and society?



Source: Targeted online survey conducted by Wavestone with DSPs. [If "No" was answered in Q16] Q18. Which additional types of digital service providers currently not in the scope of the Directive should be part of Annex III being essential for the functioning of the Union's economy and society? N for DSPs= 2

On resources

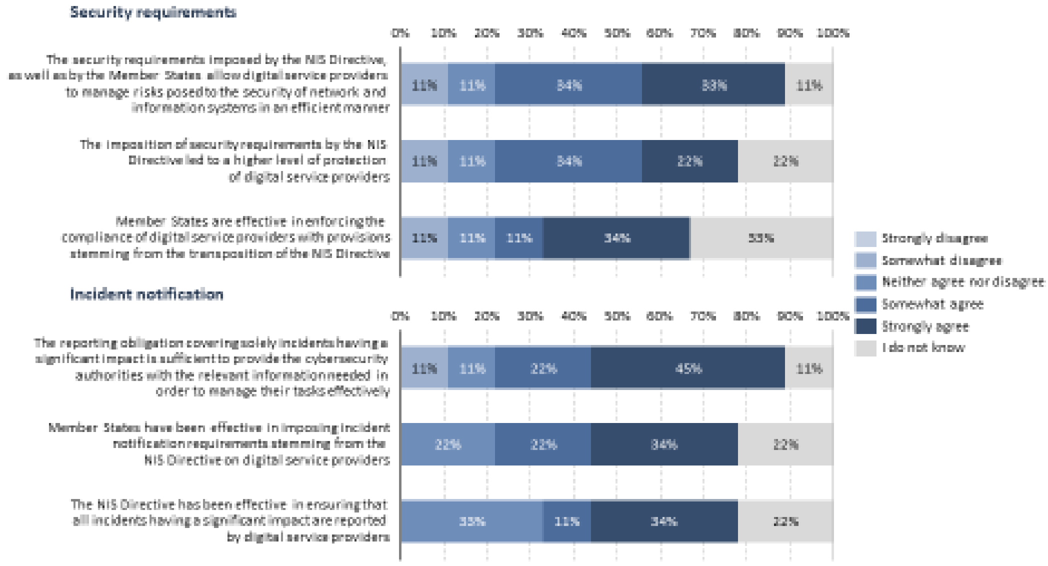
Effectiveness: Q26. To what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate?



Source: Targeted online survey conducted by Wavestone with DSPs. Q26. To what extent are the resources and staffing allocated in your organisation for the implementation of cybersecurity policies adequate? N for DSPs= 9

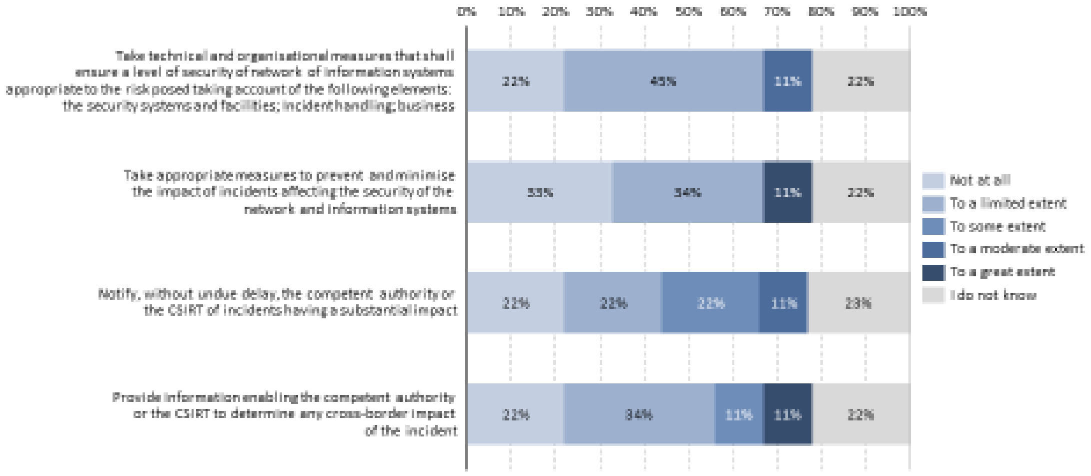
On security requirements and incident notifications

Effectiveness: Q28. To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 16 of the Directive?



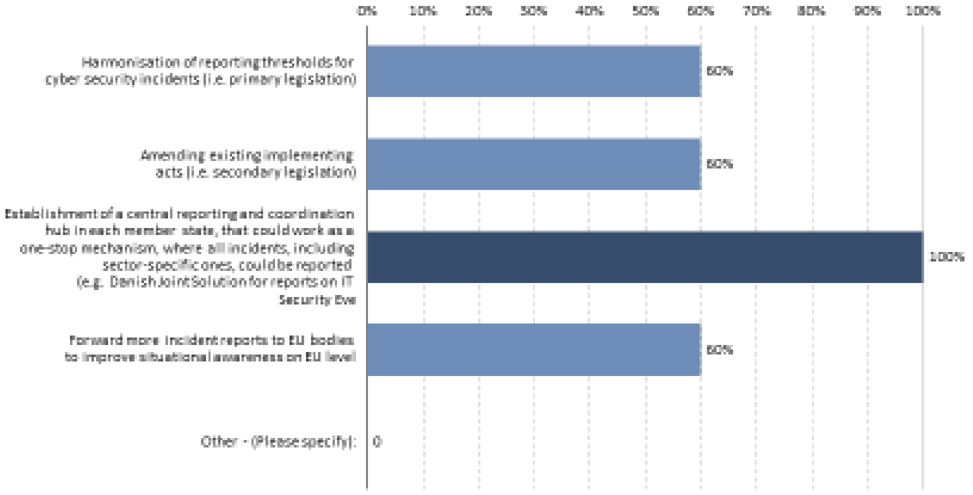
Source: Targeted online survey conducted by Wavestone with DSPs. Q28. To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 16 of the Directive? N for DSPs= 9

Effectiveness: Q29. Considering the technical and organisational requirements put forward in Article 16 of the NIS Directive to manage the risks posed to the digital service providers' security of network and information systems used in the context of offering services referred to in Annex III within the Union, to what extent did you face challenges in the implementation of the following requirements?



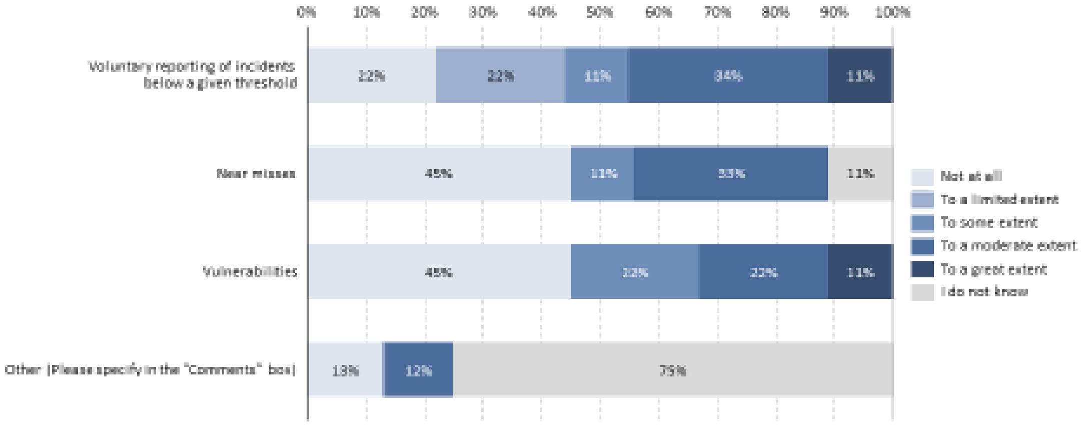
Source: Targeted online survey conducted by Wavestone with DSPs. Q29. Considering the technical and organisational requirements put forward in Article 16 of the NIS Directive to manage the risks posed to the digital service providers' security of network and information systems used in the context of offering services referred to in Annex III within the Union, to what extent did you face challenges in the implementation of the following requirements? N for DSPs= 9

Effectiveness: Conditional question [If "To a moderate extent","To a great extent" was answered in Q37] Q38. Which of the below options should be considered as means to further streamline the incident notification process?



Source: Targeted online survey conducted by Wavestone with DSPs. Conditional question [If "To a moderate extent","To a great extent" was answered in Q37] Q38. Which of the below options should be considered as means to further streamline the incident notification process? N for DSPs= 5

Effectiveness: Q39. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities?



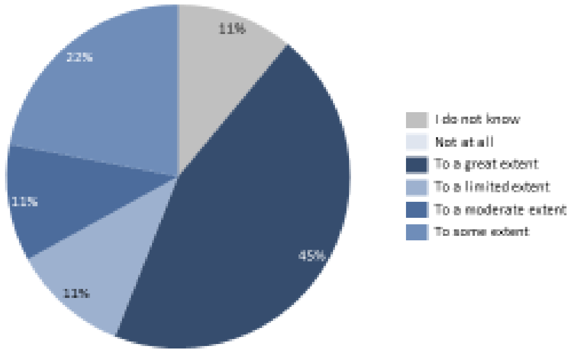
Other:

- Mandatory reporting will not provide all the necessary context.
- Vulnerabilities need to be processed in the framework of certification schemes.

Source: Targeted online survey conducted by Wavestone with DSPs. Q39. In your opinion, to what extent do you consider that new ways of reporting relevant incidents should be explored, such as voluntary reporting schemes and inclusion of additional types of cybersecurity-related incidents like "near misses" or vulnerabilities? N for DSPs= 9

On the light-touch approach for supervision

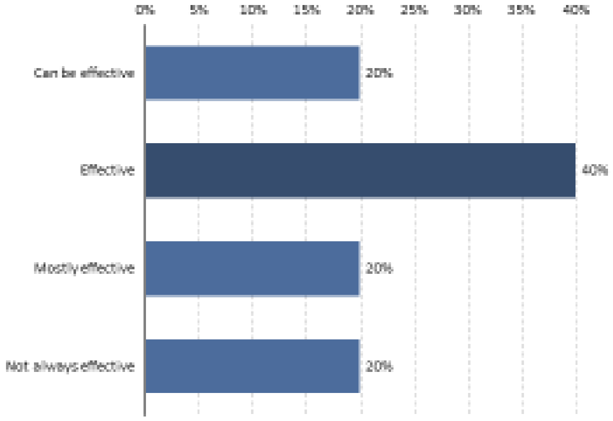
Effectiveness: Q40. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital service providers effective?



Source: Targeted online survey conducted by Wavestone with DSPs. Q40. Considering Article 17 of the NIS Directive in particular, to what extent do you consider the so-called light-touch approach (i.e. ex-post supervisory powers) applied to digital service providers effective? N for DSPs= 9

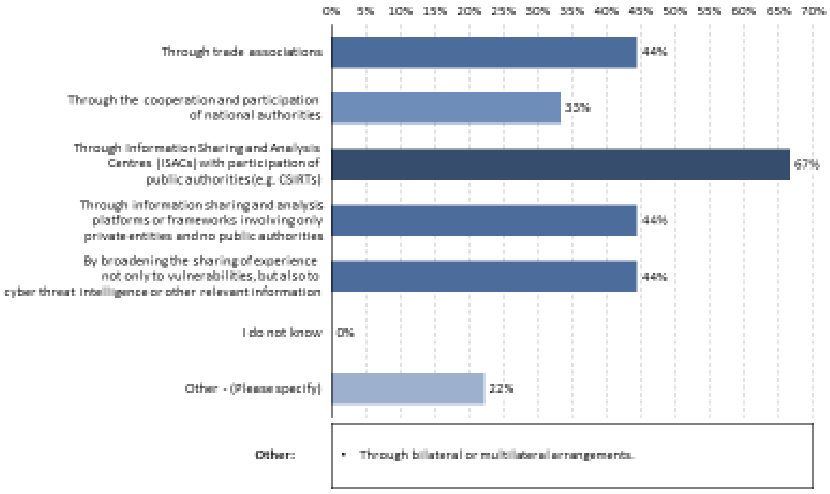
On information sharing and cooperation

Effectiveness: Conditional question : [If "Digital service provider within your sector","Digital service provider from other sectors in the same Member State","Digital service provider from the same sector from another Member State","Operators of essential service in the same Member State","Operator of essential service from another Member State","Other - (Please specify)" was answered in Q44] Q46. Could you please specify whether you consider this information sharing with other private entities effective?



Source: Targeted online survey conducted by Wavestone with DSPs. Conditional question : [If "Digital service provider within your sector","Digital service provider from other sectors in the same Member State","Digital service provider from the same sector from another Member State","Operators of essential service in the same Member State","Operator of essential service from another Member State","Other - (Please specify)" was answered in Q44] Q46. Could you please specify whether you consider this information sharing with other private entities effective? N for DSPs= 5

Effectiveness: Q47. In your view, how could a better information sharing framework between companies be promoted?



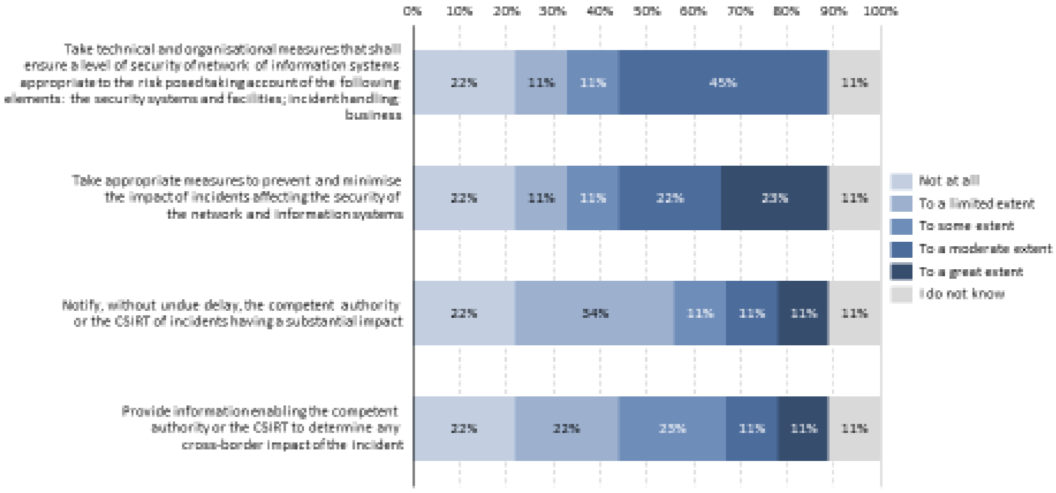
Other:

- Through bilateral or multilateral arrangements.

Source: Targeted online survey conducted by Wavestone with DSPs. Q47. In your view, how could a better information sharing framework between companies be promoted? N for DSPs= 9

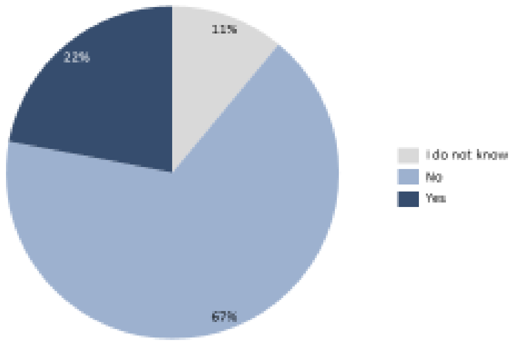
On efficiency, compliance costs and benefits

Efficiency: Q48. Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 16, to what extent were they significant for your organisation?



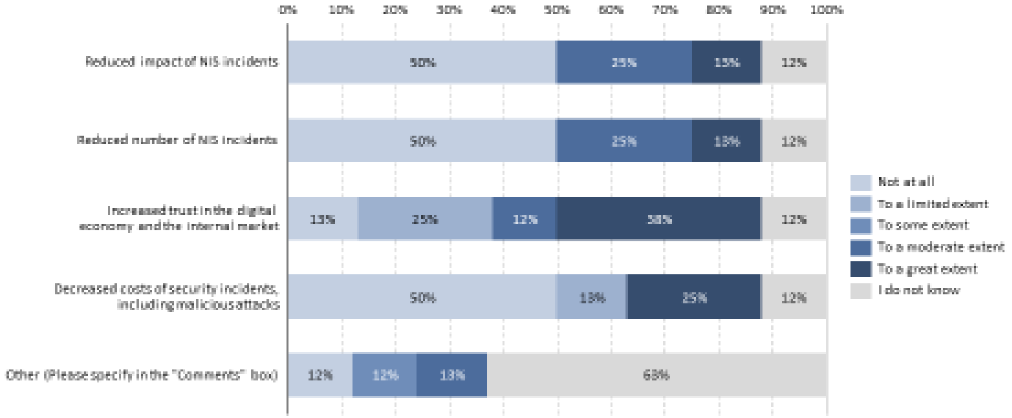
Source: Targeted online survey conducted by Wavestone with DSPs. Q48. Considering the following compliance costs with the provisions of the NIS Directive, and especially the requirements laid down in Article 16, to what extent were they significant for your organisation? N for DSPs= 9

Efficiency: Q49. Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement?



Source: Targeted online survey conducted by Wavestone with DSPs. Q49. Based on your experience, with the adoption of the NIS Directive, has your organisation been affected by the measures put forward within it in terms of additional security requirement? N for DSPs= 9

Efficiency: Q54. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case?

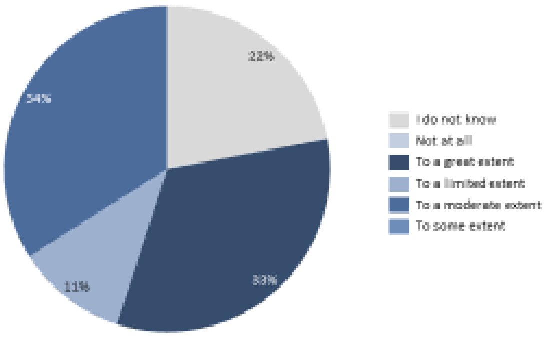


Other:

- Actual direct, derived benefits of the Directive are low.
- Enable to manage our security investment and operational security efforts.

Source: Targeted online survey conducted by Wavestone with DSPs. Q54. To what extent do the following benefits deriving from compliance with the provisions of the NIS Directive apply to your case? N for DSPs= 8

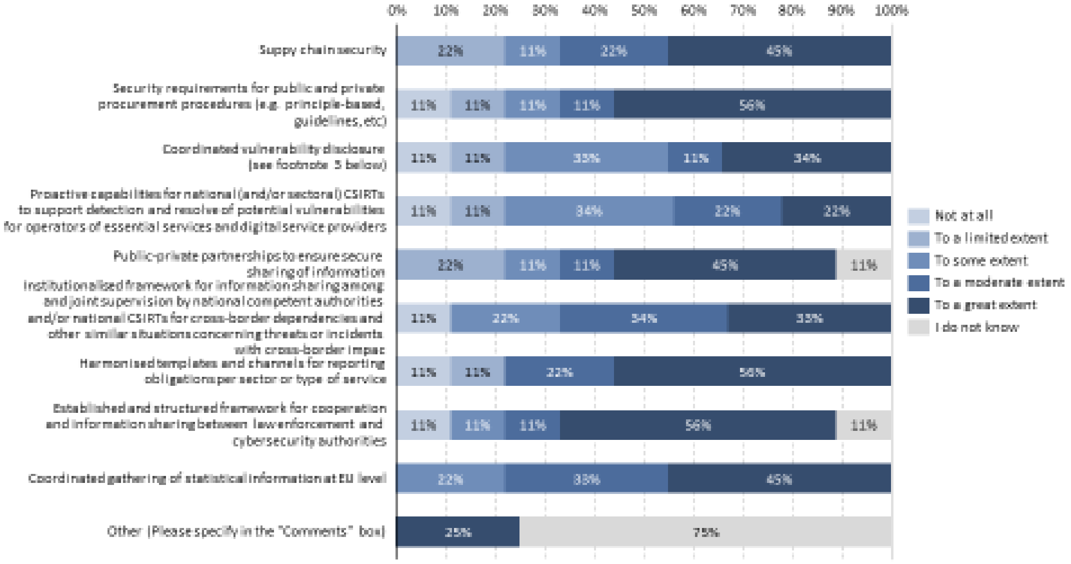
Efficiency: Q56. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought?



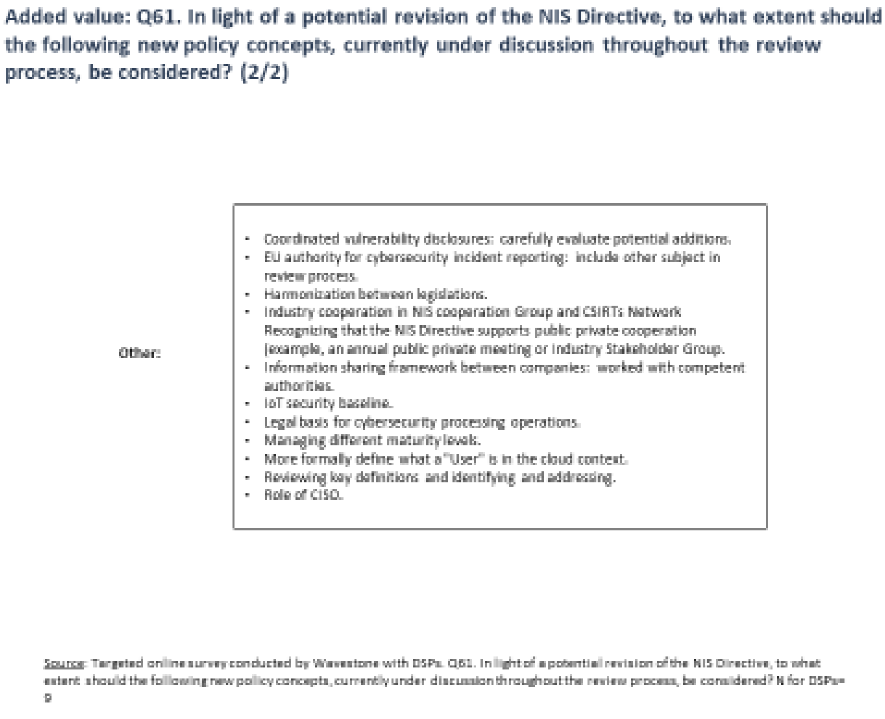
Source: Targeted online survey conducted by Wavestone with DSPs. Q56. In your view, to what extent have the costs associated with the NIS Directive been proportionate to the benefits that it has brought? N for DSPs= 9

On new policy concepts

Added value: Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? (1/2)



Source: Targeted online survey conducted by Wavestone with DSPs. Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? N for DSPs= 9



Added value: Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? (2/2)

Other:

- Coordinated vulnerability disclosures: carefully evaluate potential additions.
- EU authority for cybersecurity incident reporting: include other subject in review process.
- Harmonization between legislations.
- Industry cooperation in NIS cooperation Group and CSIRTs Network Recognizing that the NIS Directive supports public private cooperation (example, an annual public private meeting or Industry Stakeholder Group.
- Information sharing framework between companies: worked with competent authorities.
- IoT security baseline.
- Legal basis for cybersecurity processing operations.
- Managing different maturity levels.
- More formally define what a "User" is in the cloud context.
- Reviewing key definitions and identifying and addressing.
- Role of CISO.

Source: Targeted online survey conducted by Wavestone with DSPs. Q61. In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered? N for DSPs= 9

ANNEX 7: OVERVIEW OF RELATED CYBERSECURITY LEGAL ACTS AND POLICY MEASURES

The EU Cybersecurity Act[1] entered into force in June 2019, including provisions that (i) equip Europe with a framework of cybersecurity certification of products, services and processes, making sure that connected devices are reliable and trustworthy, and (ii) reinforce the mandate of the EU Agency for Cybersecurity (ENISA) to better support Member States with tackling cybersecurity threats and attacks. One of the main aims of the Cybersecurity Act is to develop a **culture of cybersecurity by design**, with security built into products and services from the start. The new cybersecurity certification framework under the Cybersecurity Act is now being implemented, with two certification schemes already in preparation, and priorities for further schemes to be identified in the Union Rolling Work Programme on cybersecurity certification.[2]

Further EU legislative and policy measures relevant to cybersecurity are also being taken in connected areas. The Commission is currently preparing a proposal, due by the end of 2020, for additional measures to enhance the protection and resilience of critical infrastructure. The Directive on the identification and designation of **European critical infrastructures**[3] (hereinafter called 'the ECI Directive') established a process to identify, designate and adopt protection measures for infrastructures that are critical from a European perspective, i.e. where their disruption would have an impact on at least two Member States, limited to the transport and energy sectors.[4] While the NIS Directive aims at ensuring that operators in the seven sectors it covers take appropriate and proportionate technical and organisational measures to manage the cybersecurity risks that their network and information systems are exposed to, irrespective of the extent of their operations over national borders, or the cross-border implications in the event of disruptions, the ECI Directive aims to enhance the general, largely physical protective arrangements surrounding designated infrastructures of cross-border significance in the energy and transport sectors alone. In 2019, the Commission conducted an evaluation of the ECI Directive, concluding that it is only of partial relevance today, in light of a range of factors including considerable changes in the context in which critical infrastructure operates in. The stated objectives of the initiative are to ensure greater coherence of the EU critical infrastructure protection approach, to include all relevant sectors providing essential services, including those defined by the NIS framework, to help Member States to achieve resilience of national infrastructures and to improve information exchange and cooperation.

Overall, since the implementation of the NIS Directive, European countries have become increasingly dependent on digital and information systems, while their networks have become ever-more interconnected. Within the Commission Work Programme 2020[5,] cybersecurity is presented as being interlinked with the digitalisation of the European

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1.

[2] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/

[3] Directive 2008/114/EC of 8 December 2008

[4] The 2006 proposal for the ECI Directive (COM(2006) 787) identified a total of 11 critical infrastructure sectors, including: energy; nuclear industry; information, communication technologies, ICT; water; food; health; financial; transport; chemical industry; space; and research facilities.

[5] COM (EU) (2020) 37 final, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Commission Work Programme 2020, 29.1.2020.

Union. Technologies used in critical sectors such as healthcare, energy, banking, and legal systems will have to be reinforced by the development of robust cybersecurity measures. Consequently, a number of other **sector-specific** legal acts or upcoming legislative proposals are also addressing cybersecurity-related aspects, as follows:

- as regards the *financial sector,* the Commission launched an initiative for a Digital Operational Resilience Framework for financial services, adopted on 24 September 2020[6]. The initiative is *lex specialis* in relation with the NIS Directive, setting out consolidated, simplified and upgraded ICT risk requirements throughout the financial sector to ensure that all participants of the financial system are subject to a common set of standards to mitigate ICT risks for their operations.

- in the *energy sector*, the Risk Preparedness Regulation[7] inter alia sets a framework to ensure that Member States prevent and manage crisis situations in cooperation with each other in a spirit of solidarity. This Regulation complements the NIS Directive *"by ensuring that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans"*.[8] The same applies to the Regulation[9] concerning measures to safeguard the security of gas. Both instruments are accompanied by a Commission Recommendation[10] on cybersecurity in the energy sector providing sector-specific guidance. Furthermore, as part of the development of network codes and guidelines for the period 2020-2023 for electricity and for 2020 for gas, a Network Code for the cybersecurity of cross-border energy flows is being established[11]. In this context, sector-specific rules for cyber security aspects of cross-border electricity flows should allow the electricity networks to address potential cyber threats so that clean energy is fit for the digital age

- in the *transport sector*, additional initiatives are being put forward by the Commission and relevant EU bodies, with the aim of increasing the robustness of services against cyberattacks. Such initiatives regard, for example, the *aviation sector*, where, the EU adopted detailed rules for cybersecurity in the aviation security domain[12]. The EU Aviation Safety Agency (EASA) is preparing an opinion to be submitted to the European Commission in order to amend aviation safety legislation with cybersecurity provisions requiring the mandatory introduction of an Information Security Management System. In *maritime transport*, EU security legislation[13] already contains provisions relating to cybersecurity. Cybersecurity is also part of the EU Maritime Security Strategy dating from 2014[14], with an action plan revised in 2018. In addition, the

[6] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, COM(2020) 595 final.

[7] Regulation (EU) 2019/941.

[8] Recital 7 of Regulation (EU) 2019/941 (Risk Preparedness Regulation).

[9] Regulation (EU) 2017/1938.

[10] C(2019)2400 final of 3 April 2019.

[11] 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,

[12] Commission Implementing Regulation (EU) 2019/1583

[13] Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security, Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

[14] http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT

Commission, the EU Aviation Safety Agency (EASA), the European Maritime Safety Agency (EMSA) and ENISA rely on a series of expert groups gathering representatives from the different modes of transport to exchange viewpoints and ideas on cyber security threats, challenges and solutions. For example, cybersecurity is regularly discussed between the Commission, Member States and stakeholders at the level of transport security committee meetings for each mode[15]. EASA chairs a European Strategic Coordination Platform (ESCP) including key industry stakeholders, Member States and EU Institutions. This has led to the first common EU strategy for cybersecurity in aviation. It is also supporting the creation of a European Centre for Cybersecurity in Aviation (ECCSA) and providing the initial operational capabilities currently in collaboration with CERT-EU. With the support of ENISA, the Transport Resilience and Security Expert Group (TRANSSEC) was also set up, gathering experts from the transport sector to exchange viewpoints and ideas on cyber security threats, challenges and solutions.

As regards *electronic communication networks and services*, the cybersecurity aspects in relation to these are now regulated, starting 21 December 2020, by the European Electronic Communications Code (EECC). The NIS Directive excludes from its security and notification requirements undertakings providing public communications networks or publicly available electronic communications services, which are subject to the requirements of Articles 13a and 13b of Framework Directive 2002/21/EC, which is repealed with effect from 21 December 2020.[16] The Connectivity Package, which reshapes telecoms regulation, redefines the term 'electronic communications network' in the EECC. A so-called 'Article 13a group' made of Member States representatives and supported by ENISA, distinct from the Cooperation Group, is covering the cybersecurity policy aspects related to electronic communication networks and services and would continue to do so absent any changes to the NIS Directive. Seven Member States added the **electronic communication networks and services** to the scope of the NIS-related rules.

The table below developed by the NIS review study points to the specific provisions of the NIS Directive and other EU legislation that are inter-related, notably as regard the security requirements and reporting obligations.

[16] The Connectivity Package, which reshapes telecoms regulation, redefines the term 'electronic communications network' in the EECC.

NIS Directive - External coherence with other EU interventions			
European Electronic Communications Code (EECC)			
Provisions	**NIS Directive**	**EECC Directive**	**Analysis**
Security notification requirements	**Article 14(1) NIS Directive**: requires Member States to ensure that the OES *'take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.'*	**Article 40 EECC**: requires Member States to ensure that providers of electronic communications networks or of publicly available electronic communications services *'take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and systems.'*	Both provisions take a **risk-based approach** when implementing security measures. While the **NIS Directive** refers to '*security of network and information systems*', **the EECC** refers to '*security of networks and services*' with both defining security as '*the ability of*' network and information systems/electronic communications networks and services *'to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality*' of stored or transmitted or processed data/of those networks and services.

NIS Directive - External coherence with other EU interventions			
	Article 14(3) NIS Directive *require Member States to ensure that security incidents having a significant impact on the continuity of the essential services/on the operation of networks or services, are reported without undue delay.*	***Article 40(2) EECC*** *require Member States as well to ensure that security incidents having a significant impact on the continuity of the essential services/on the operation of networks or services, are reported without undue delay.*	*Overall,* ***no divergences between the framework on security measures in the NIS Directive and EECC could be identified****. However, as a mere formality, there should be alignment as regards the notion of 'incident' in the NIS Directive and 'security incidents' in the EECC, although the definitions are similar.* *In addition, there could be a potential coherence issue for reporting schemes related to Internet Service Providers (ISPs) between* ***Article 14 NIS Directive*** *and* ***Article 40 EECC*** *if the new reporting scheme implemented under Article 40 EECC was not followed: one incident could be reported under two different requirements.*

Electronic identification and trust services for electronic transactions (eIDAS Regulation)			
Provision	***NIS Directive***	***eIDAS Regulation***	***Analysis***
Security notification requirements	***Article 1(3) of the NIS Directive****, require that the security and notification requirements provided for in the NIS Directive shall not apply to trust service providers which are subject to the requirements of Article 19 eIDAS Regulation.*	***Articles 19(1) and 19(2) eIDAS Regulation*** *require inter alia that providers of trust services take appropriate security measures to mitigate risks posed to the security of their trust services and notify, without undue delay but in any event within 24 hours after becoming aware of it, the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that 'has a significant impact on the trust service provided or on the personal data maintained therein'.*	*Coherence issues may arise when digital certificates are used for authentication in services that fall under the scope of the NIS Directive. This is likely with regard to financial services or cloud services. In addition, under the eIDAS Regulation the reporting time frame is 24 hours, whereas NIS Directive requires it to happen 'without undue delay'.*

General Data Protection Regulation (GDPR)			
Provision	***NIS Directive***	***GDPR Regulation***	***Analysis***
Security notification requirements	***Articles 8(6)*** *and* ***15(4) NIS Directive*** *require the competent authorities and single point of contact under the NIS Directive to consult and cooperate with national data protection authorities*	***Article 33(1) GDPR*** *require data controllers to notify a personal data breach to the supervisory authority without undue delay, at the latest within 72 hours after becoming aware of it. In addition, if the data breach is likely to result in a high risk to the rights and freedoms of natural persons and non of the conditions described in Article 33(3) applies, controllers are required to communicate the personal data breach to the data subject without undue delay.*	*The difference to the NIS Directive is that the GDPR is only applicable to* ***incidents*** *that concern* ***personal data*** *and upon the condition that the data breach results to a risk to the rights and freedoms of natural persons. Even if one may, in theory, distinguish between incidents falling under the GDPR and such falling under the NIS Directive, in practice,* ***most security incidents will involve*** *(at least potentially)* ***some personal data. However since the legal instruments have different objectives legal instruments.*** *This means that OESs and DSPs will have to* ***report*** *as subset of security incidents* ***to both competent authorities*** *in order to ensure compliance with both regulatory requirements.*

Payment services in the internal market (PSD2 Directive)			
Provision	***NIS Directive***	***PSD2 Directive***	***Analysis***
Security notification requirements	***Article 14(5) NIS Directive*** *requires the competent authority to notify the relevant authorities in other Member States if the incident is of relevance for them.*	***Article 95(1) PSD2*** *requires payment service providers to adopt appropriate mitigation measures and controls mechanisms relating to the payment services they provide. It also requires the establishment and maintenance of effective incident management procedures including for the detection and classification of major operational and security incidents.* ***Article 96 PSD2*** *establishes an incident notification scheme, which foresees that payment service providers 'shall report without undue delay any major operational or security incident to their competent authority in the Member State'.* ***Article 96 PSD2*** *also requires payment services providers to inform its payment service users where the incident has or may have an impact on the financial interests of the user.*	*Payment service providers are encompassed within* ***Annex II of the NIS Directive*** *as* ***part of the financial services sector****. However, as Article 1(7) NIS Directive foresees that where a sector-specific Union legal act requires an OES either to ensure the security of his network and information systems or to notify incidents, that act shall apply provided that the requirements are at least equivalent. Considering that the security and notification requirements prescribed in* ***Articles 95 and 96 PSD2 are equivalent****, these provisions are lex specialis to the NIS Directive. Hence, there is* ***no coherence issue****.*

In 2018, the Commission put forward a proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research **Competence Centre** and the Network of National

Coordination Centres[17]. The initiative aims to better target and coordinate available funding from the EU budget and Member State contributions for cybersecurity cooperation, capacity and infrastructure building as well as research and innovation. The competence centre should become the main body that would manage EU financial resources dedicated to cybersecurity research under two proposed programmes – **Digital Europe and Horizon Europe** – within the next multiannual financial framework, for 2021-2027. These programmes are pooling more EU and national funding for cybersecurity research, innovation and infrastructure, cyber defence, and the EU's cybersecurity industry. The Commission proposed to invest €2 billion specifically on cybersecurity. Trialogue negotiations are currently ongoing as part of the adoption procedure of the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

In 2017, the Commission adopted a Joint Communication to the European Parliament and the Council on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, setting a **common approach to cybersecurity with resilience-building**, rapid response and effective deterrence.[18] Proposals to support this through building essential capacities are pending adoption.[19]

Given the ongoing roll-out of the 5G infrastructure across the EU and the potential dependence of many critical services on 5G networks, the consequences of systemic and widespread disruption would be particularly serious. The process put in place by the Commission's 2019 Recommendation on the **Cybersecurity of 5G networks**[20] has led to Member State action on the measures set out in a 5G toolbox, as reflected in the report on the implementation of the Toolbox adopted in July 2020[21]. The Recommendation foresees its review in the last quarter of 2020.[22]

EU institutions, bodies and agencies (EU-I), with CERT-EU and ENISA's help, are considering how to prepare better for future incidents and crises, including through the implementation of the Blueprint Recommendation, the development of the Member State **Cyber Crises Liaison Organisation Network ("CyCLONe") and Cyber Europe incident and crisis management exercises** for the public and private sectors. CyCLONe is notably intended to: (i) facilitate trust building, preparedness, situational awareness and crisis management between national relevant competent authorities; (ii) interact with both the technical (i.e., CSIRT Network) and the EU political level on how to manage large-scale cybersecurity incidents and crises; (iii) support national and EU political level to make an informed decision in large-scale cybersecurity incidents and crises, while avoiding unnecessary escalations to EU level political crisis mechanisms when the

[17] COM (2018) 630 final, of 12.9.2018: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research

[18] JOIN (2017) 450 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2017%3A450%3AFIN

[19] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, COM(2018) 630 final, 2018/0328 (COD

[20] OJ L 88, of 29.3.2019, p 42 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0534

[21] Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity; https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

[22] Commission Recommendation on the Cybersecurity of 5G networks C(2019) 2335 final; Commission. Communication on the Secure 5G deployment in the EU: Implementing the EU toolbox COM(2020) 50 final.

impacts can be dealt with by the operational layer. The Commission has also identified the need for a **Joint Cyber Unit** to provide structured and coordinated operational cooperation. Building on the implementation of the Blueprint recommendation[23], the Joint Cyber Unit could build trust between the different actors in the European cybersecurity ecosystem and offer a key service to Member States from technical, operational and political level and integration of EUI, MS, CyCLONe SOPs, as well as potential synergies with the PESCO projects.

Cybersecurity is also an important component of the ***EU framework for countering hybrid threats***[24], since the adoption of the first Joint Communication on countering hybrid threats a European Union response in 2016, establishing the link with the NIS framework and highlighting the importance of the convergence of risk management approaches and public-private cooperation[25]. Three sectors were prioritised in this context: energy, transport and finance.

In 2013, Europol set up the **European Cybercrime Centre (EC3)**[26] to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. EC3 is involved in high-profile operations and on-the-spot operational-support deployments. EC3 publishes the annual Internet Organised Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime.

By the end of 2020, the Commission will also adopt a **new cybersecurity strategy – a cybersecurity charter for the EU**, setting out a comprehensive vision, including the role that the NIS legal framework should play.

[23] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239, 19.9.2017.

[24] Defined as a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.

[25] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats a European Union response JOIN/2016/018 final.

[26] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

ANNEX 8: OVERVIEW OF POLICY OPTIONS

Specific policy objectives (SPO)	**Policy options**			
	Policy option 0 – *maintaining the status quo*	**Policy option 1 – *non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 – *Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 – *Systemic and structural changes to the NIS Directive (new directive)***
SPO1: Ensure that entities in all sectors that are dependent on network and information systems and that provide key services to the economy and society as a whole are required to take cybersecurity measures and report incidents with a view to increasing the overall level of cyber resilience throughout the internal market	Maintaining the scope, requirements and obligations. Continue existing work of the Cooperation Group and the CSIRTs network.	Maintaining the scope, requirements and obligation, while providing sector-specific guidance via the Cooperation Group or by the Commission directly	Bring additional sectors, subsectors and services under the scope within the existing two categories covered by the NIS Directive (OES and DSP)	Bring additional sectors, subsectors and services under the scope, while further refining and simplifying the categories of entities covered by the NIS framework depending on their importance and criticality (i.e. essential and important), and consequently differentiating the particular requirements and supervisory regime imposed on those.
SPO2: Ensure that all		Guidelines on OES	Harmonize essential	Abandon identification and

Specific policy objectives (SPO)	**Policy options**			
	Policy option 0 – *maintaining the status quo*	**Policy option 1 – *non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 – *Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 – *Systemic and structural changes to the NIS Directive (new directive)***
entities that are active in sectors covered by the NIS legal framework and that are similar in size and have a comparable role are subject to the same regulatory regime (are either inside or outside the scope) no matter under which jurisdiction they fall within the EU		identification and coverage of DSPs	services and identification thresholds.	introduce uniform criteria for all entities operating in the sectors and subsectors or providing services covered under the NIS scope, excluding micro or small size enterprises. Entities which are micro or small, but provide services as a sole provider in a Member State or a potential disruption of which could have an impact on the public safety or health would also fall within the NIS scope. Member States would also be able to include in the NIS scope micro and small-size entities in the sectors and services covered by the NIS framework justified on the basis of their importance at

Specific policy objectives (SPO)	**Policy options**			
	Policy option 0 – ***maintaining the status quo***	**Policy option 1 –** ***non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 –** ***Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 –** ***Systemic and structural changes to the NIS Directive (new directive)***
				regional or national level for that particular sector or service or for other interdependent sectors.
			Introduce clearer and more explicit definitions for DSPs. Further clarify the jurisdiction rules. Establishing equal footing for OESs and DSPs.	Establish equal footing for all entities of same criticality/importance, while removing the differences in regulatory regime between the entities which are currently qualified as operators of essential services or digital service providers. Establish a registry of digital service providers operating cross-borders. Further clarify the jurisdiction

Specific policy objectives (SPO)	Policy options			
	Policy option 0 – *maintaining the status quo*	**Policy option 1 – *non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 – *Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 – *Systemic and structural changes to the NIS Directive (new directive)***
				rules.
SPO3: Ensure that all entities that are active in sectors covered by the NIS legal framework must follow aligned obligations based on the concept of risk management when it comes to security measures and must report incidents based on a uniform set of criteria		Guidelines on security and incident reporting requirements	Harmonize security and incident reporting requirements Introduce more explicit incident reporting requirements	Introduce uniform and explicit security and incident reporting requirements, potentially directly applicable to the relevant entities. Introduce more explicit reporting obligations concerning incidents, including towards ENISA.
SPO4: Ensure that competent authorities enforce the rules laid		Guidelines on supervision and	Establish principles for application of supervisory measures and penalties,	Establish principles, as well as a more granular list of minimum requirements, for

Specific policy objectives (SPO)	**Policy options**			
	Policy option 0 – ***maintaining the status quo***	**Policy option 1 –** ***non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 –** ***Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 –** ***Systemic and structural changes to the NIS Directive (new directive)***
down by the legal instrument more effectively through aligned supervisory and enforcement measures		enforcement	including general conditions for the application of administrative fines.	supervisory measures and enforcement, tailor-made for each category of entities, depending on the level of importance/criticality of the services provided. Establish general conditions for application of administrative fines and a minim level thereof. Establish a peer-review system, including on the implementation of supervisory measures and enforcement. Introducing liability rules for natural persons responsible for or acting as a representative of the legal person.

Specific policy objectives (SPO)	**Policy options**			
	Policy option 0 – *maintaining the status quo*	**Policy option 1 – *non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 – *Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 – *Systemic and structural changes to the NIS Directive (new directive)***
		Guidelines on DSPs supervision	Subject DSPs to the same rules as OES (i.e. remove the light-touch approach and introduce full supervision, including *ex-ante,* for DSPs).	Subjecting entities (both operators and digital service providers) qualified under the same category (i.e. essential or important) to the same regulatory regime, including supervision and enforcement. Important entities would be subject to a light-touch regulatory regime (i.e. only *ex-post* supervision and lighter requirements on penalties).
SPO5: Ensure a comparable level of resources across Member States allocated to competent authorities that would allow		Incentivise Member States, via the Cooperation Group, and through peer pressure to adequately fund their competent	Require Member States to take the necessary measures to ensure that the competent authorities have the technical, financial and human resources to fulfil their mandate, and in	Set up a peer-review mechanism to assess, among others, the capabilities of the Member States.

Specific policy objectives (SPO)	**Policy options**			
	Policy option 0 – *maintaining the status quo*	**Policy option 1 – *non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 – *Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 – *Systemic and structural changes to the NIS Directive (new directive)***
them to fulfil the core tasks laid out by the NIS framework		authorities and other relevant structures, such as the CSIRTs	particular their supervisory and guiding roles	
SPO6: Ensure that essential information is exchanged between Member States by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents and by developing a Union joint operational crisis response capacity	Continue existing work of the Cooperation Group and the CSIRTs network	Further develop Standard Operational Procedures (SOPs) by the Cooperation Group and the CSIRTs network. Launching CyCLONe, without a set legal framework.	Mandate or incentivize information sharing for competent authorities and companies (ISACs, PPPs).	Set up specific mandatory mutual assistance and cooperation mechanism when cross-border elements are involved. Incentivise voluntary information sharing through ISACs and PPPs. As part of the national cybersecurity strategy, Member States will be required to develop a policy framework on co-ordinated vulnerability disclosure and designate a national CSIRT as a

Specific policy objectives (SPO)	**Policy options**			
	Policy option 0 – ***maintaining the status quo***	**Policy option 1 –** ***non-legislative measures to align the transposition of the NIS Directive***	**Policy option 2 –** ***Limited changes to the current NIS Directive for further harmonization***	**Policy option 3 –** ***Systemic and structural changes to the NIS Directive (new directive)***
				coordinator and facilitator. Adding the role of observatory of the state of cybersecurity in the Union to ENISA. Introducing annual/biennial/regular reports on the state of cybersecurity in the EU.
				Introducing a crisis management framework, for both national and EU levels, including institutionalising CyCLONe.

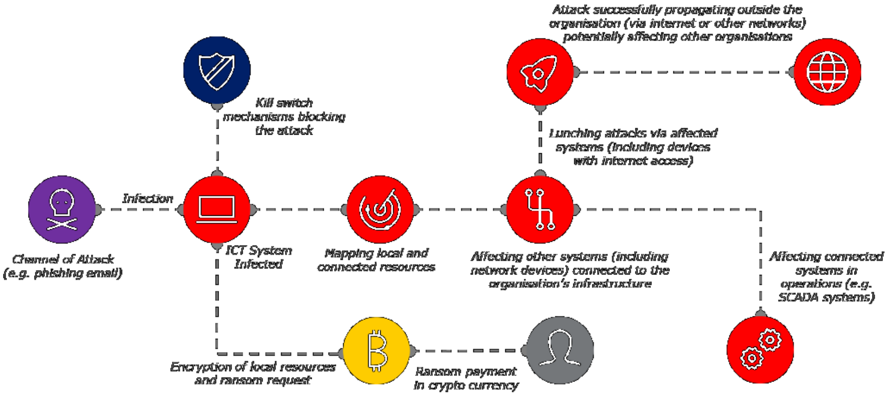
ANNEX 9: CROSS-SECTOR AND CROSS BORDER PROPAGATION OF INCIDENTS

The 2017 WannaCry ransomware outbreak infected over 230,000 computers in 150 countries on the first day alone[27]. The economic impact of the WannaCry incident is estimated in the order of hundreds of million euros with some cyber risk modelling analysts placing the losses in the order of billions. *For more additional examples and arguments on cross sector and cross border propagation of incidents see annex 10.*

The SamSam ransomware attacks affected different organisations across sectors, the ransomware encrypts data and demand a huge ransom payment in Bitcoin in exchange for the decryption keys. SamSam has attacked different large organisations across sectors, including Transport (e.g. COSCO attack) and Health. As mentioned by the above-referenced ENISA good practices report, SamSam has earned its creator(s) more than 5 million euros since late 2015, a figure that does not take into account revenue losses and system restore costs.

The July 2020 JRC Report[28] also mentions the example of the 2007 coordinated cyber attacks on Estonia, which targeted governmental institutions and bodies, financial entities, telecommunication infrastructure and newspapers: *'a surge of DDoS attacks lasting several weeks caused disruptions at institutional sites and in national online public services and communications, impacting the normal functioning of the national government and society (Schmidt, 2013). These attacks were not highly sophisticated and, due to their nature, did not create any lasting damage to Estonia's digital infrastructure. However, they demonstrated how cyber attacks taking advantage of the digital transformation of governments and society could severely harm an entire country (Joubert, 2012)'.*

The chart below was drafted by ENISA in its good practices on the interdependencies between the OESs and DSPs to illustrate how cross sector and cross border propagation of incidents may occur.[29]


Attack successfully propagating outside the organisation (via internet or other networks) potentially affecting other organisations
Kill switch mechanisms blocking the attack
Lunching attacks via affected systems (including devices with internet access)
Infection
Channel of Attack (e.g. phishing email)
ICT System Infected
Mapping local and connected resources
Affecting other systems (including network devices) connected to the organisation's infrastructure
Affecting connected systems in operations (e.g. SCADA systems)
Encryption of local resources and ransom request
Ransom payment in crypto currency

ENISA, in its 2018 good practices, has also pointed to a number of increasing dependencies in certain sectors, such as in the example below concerning the transport sector.[30]

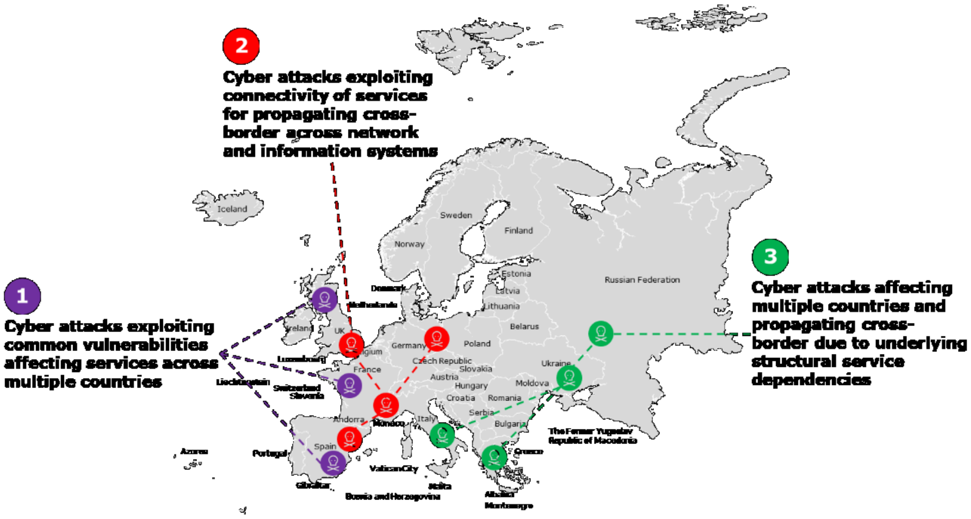
[27] Department of health & Social Care (NHS) UK, 2018.

[28] JRC, July 2020: *Cybersecurity – Our Digital Anchor, a European perspective*

[29] Figure 3, page 12, https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps

The JRC Report[31] highlights that *'From big data to hyperconnectivity, from edge computing to the IoT, to artificial intelligence (AI), quantum computing and blockchain technologies, the 'nitty-gritty' details of cybersecurity implementation will always remain field-specific due to specific sectoral constraints. This brings with it inherent risks of a digital society with heterogeneous and inconsistent levels of security. To counteract this, we argue for a coherent, cross-sectoral and cross-societal cybersecurity strategy which can be implemented across all layers of European society.'*

Furthermore, ENISA's 2018 good practices on interdependencies between OES and DSP looked, among others, into cross-border interdependencies, illustrating the types of cyberattacks with cross-border implications in the figure copied below.[32]


2
Cyber attacks exploiting connectivity of services for propagating cross-border across network and information systems
1
Cyber attacks exploiting common vulnerabilities affecting services across multiple countries
3
Cyber attacks affecting multiple countries and propagating cross-border due to underlying structural service dependencies
Iceland
Sweden
Finland
Norway
Estonia
Russian Federation
Denmark
Latvia
Netherlands
Lithuania
Ireland
UK
Belarus
Belgium
Germany
Poland
Luxembourg
Czech Republic
Slovakia
Ukraine
France
Austria
Hungary
Moldova
Liechtenstein
Switzerland
Slovenia
Croatia
Romania
Serbia
Andorra
Monaco
Italy
Bulgaria
The Former Yugoslav Republic of Macedonia
Azores
Portugal
Spain
Greece
Vatican City
Gibraltar
Malta
Bosnia and Herzegovina
Albania
Montenegro

Cross-border dependencies therefore pose particular challenges, and would require an effective cross-border cooperation and information sharing.

[30] Figure 6, page 17, idem.

[31] JRC, July 2020: *Cybersecurity – Our Digital Anchor, a European perspective.*

[32] Figure 8, page 21.

Annex 10: Extract from the interim results of the NIS review study on a modelling for costs and benefits

Note: This is an estimation of costs and benefits which will be incorporated in the final report of the NIS review study[33] *due in December 2020/January 2021. The estimation of costs and benefits follows Tool#59 of the EU Better Regulation Tool*[34].

The main benefit for an intervention aiming to achieve a high level of cyber resilience is **the reduction in cyber incidents** compared to the baseline scenario[35].

$$\begin{aligned} Economic\ benfit\ for\ option\ i &= Reduction\ in\ cost\ of\ cyber\ incidents \\ &= cost\ of\ cyber\ incidents\ in\ baseline \\ &- cost\ of\ cyber\ incident\ in\ option\ i \end{aligned}$$

The monetary value of cyber incidents relies on different sources based on past incidents. A comprehensive dataset with cyber incident and economic impact is not available. As noted by the Hague report[36], determining the overall impact of cyber attacks is challenging because there are different reports on cybercrime such as malware, social engineering and fraud to name a few, each source with different methodologies. The lack of a coherent and consistent methodology with standard indicators makes the task challenging. For example, there is abundant anecdotical data of incidents or estimations but varies by scope (sectors, countries, regions), and data by sector can varies remarkably.

However, for the purpose of our estimation at societal level, we need evidence from Europe as a whole. The 2015 Ponemon Institute study on the costs of cybercrime provides the median annualized costs of cybercrime which amounts to USD 5.5 million (EUR 4.63 million).[37] Moreover, there **were almost 450 cybersecurity incidents in 2019 involving** European critical infrastructures like health, finance and energy according to Eurostat[38].

Based on the median annualized cost of cyber incidents and the number of incidents per year, Figure 1.1 below displays a linear extrapolation of costs of cyber incidents followings four assumptions:

Based on the average cost of cyber crime and the number of incidents per year, Figure 1.1 below displays a linear extrapolation of costs of cyber incidents followings four assumptions:

1. The annual growth rate of incidents in the baseline scenario follows annual rate of growth in the patterns of digitisation (3%);
2. The annual fall of incidents in option 2 is a conservative 3%;

[33] 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.

[34] https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-59_en_0.pdf

[35] Note that as the cost in the baseline is higher than otherwise the difference gives a negative magnitude, but a negative cost is a benefit

[36] https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf

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

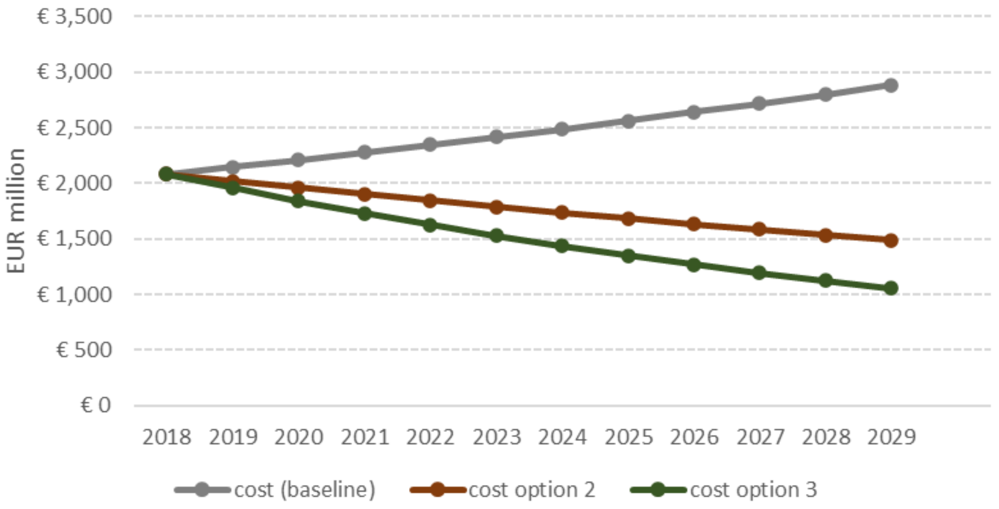
[38] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

3. The annual fall of incidents in option 3 is double compered to option 2, namely, 6%
4. The average cost of a cyber incident stays the same in time;
5. We set to 450 the number of incidents in 2018 according to Eurostat figures;

Such assumptions are the most conservative.

[…]

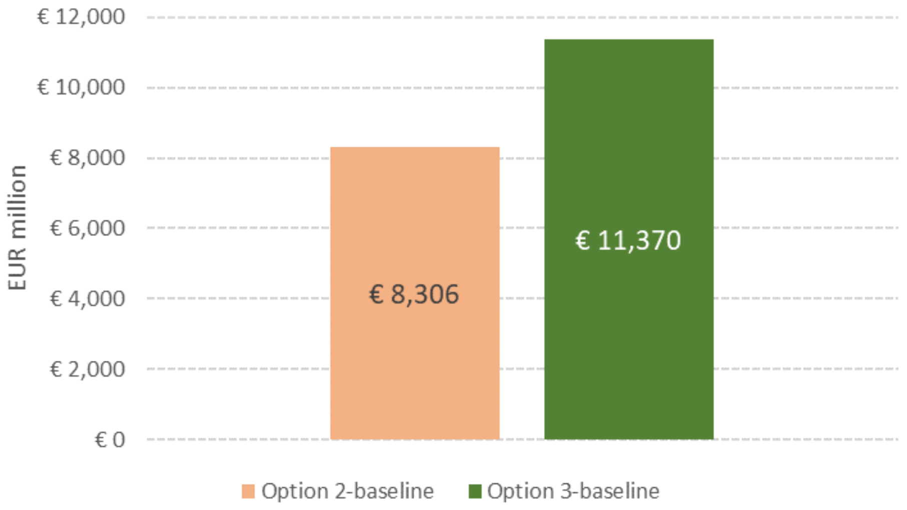
Figure 1.1 The costs of cyber-incidents across scenarios in EUR million (2018-2029)



Source: own elaboration

The expected benefit in option 2 and option 3 are given by the difference of the cost of cyber incidents compared to the baseline over the 10-years period.

Figure 1.2 Saving in cyber incident per option compared to the baseline



Source: own elaboration

In sum, option 3 is the most impactful with a reduction in cost of cyber incidents by EUR 11.3 billion while option 2 by EUR 8.3 billion.

ANNEX 11: LIST OF INDICATORS TO MONITOR HIGH-LEVEL PROGRESS TOWARDS GENERAL OBJECTIVES

General objectives	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
Increase the level of cyber resilience of a comprehensive set of businesses operating in the European Union across all relevant sectors	1. Comparable ICT security spending across sectors and Member States 2. Results of random assessments at EU level of cybersecurity capabilities and implementation of cybersecurity policies of 2 key entities per Member State per NIS sector and types of service in at least five Member States (*part of the State of Cybersecurity in the Union Report)* 3. Findings of peer-review mechanism visits as regards the level of NIS compliance and cybersecurity capabilities across the EU 4. Overall set of indicators across the EU of the regular business resilience survey	1. Sector-specific ICT security spending as a percentage of ICT spending across Member States deviating with less than 1% from the average sectorial security spending 2. Positive findings on compliance with NIS requirements and level of capabilities *(i.e. technical, financial and human)* random sector or service-specific assessments of cybersecurity policies of key entities in at least five Member States 3. Regular progress found by peer-	1. ENISA data set based on outcomes of framework contract on investment on cybersecurity 2. Data gathered for the report on the State of Cybersecurity in the Union (ENISA) 3. Peer-review reports 4. Annual cyber resilience business survey	1. Annual 2. Every two years 3. Annual (different sets of Member States per year) 4. Annual

General objectives	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
		reviews in the level of cybersecurity capabilities across the EU and rate of follow-up of experts' recommendations 4. Cumulative positive trend at EU level on all indicators covered by the regular business resilience survey		
Reduce inconsistencies in the resilience across the internal market in the sectors already covered by the Directive	1. ICT security spending per sector and type of service per Member State as a percentage of IT spending and revenues 2. Results of comparative assessments per sectors and types of services per Member State of cybersecurity capabilities and compliance with the NIS framework (*part of the State of Cybersecurity in the Union Report)* 3. Findings of peer-review mechanism visits as regards the level of NIS compliance and cybersecurity	1. Even and steady ICT security spending per sector and type of service at Member State level correlated to the evolution of overall revenue/turnover in that sector/type of service per Member State 2. Even and steady level of	1. ENISA data set based on outcomes of framework contract on investment on cybersecurity 2. Data gathered for the Report on the State of Cybersecurity in the Union (ENISA)	1. Annual 2. Every two years 3. Annual (different sets of Member States per year) 4. Annual

General objectives	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
	capabilities across the EU 4. Comparative sets of indicators per Member State of the regular business resilience survey	cybersecurity capabilities and NIS compliance in sector or service-specific assessments per Member State 3. Regular progress at the level of each Member State found by peer-reviews	3. Peer-review reports 4. Annual cyber resilience business survey	
Improve the level of joint situational awareness and the collective capability to prepare and respond	1. Regularity and comprehensiveness of threat assessments and state of cybersecurity in the union reporting 2. Completeness of Member States notifications of relevant NIS data to the Commission and ENISA (e.g. incident notifications, discovered vulnerabilities, exchanges of information, instances when mutual assistance mechanism was applied, etc.) 3. Number of time the mutual assistance mechanism was triggered in cross-border cases	1. Accurate threat assessment and comprehensive State of Cybersecurity in the Union Report 2. Complete Commission and ENISA databases on NIS relevant data 3. Frequent use of mutual assistance mechanism in cross-border cases, including joint supervisory actions.	ENISA and Commission reports	Annual

ANNEX 12: LIST OF INDICATORS TO MONITOR PROGRESS TOWARDS SPECIFIC OBJECTIVES

Specific Objectives	*Operational objectives*	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
SPO1*: Ensure that entities in all sectors that are dependent on network and information systems and that provide key services to the economy and society as a whole are required to take cybersecurity measures and report incidents with a view to increasing the overall level of cyber resilience throughout the internal market*	Ensure awareness of all entities per sector/ service per Member State of inclusion of the NIS scope and corresponding requirements.	Type and number of entities per sector/service per Member State for which supervisory measures were applied by Member States and notification obligations received.	Entities from all sectors and services covered under NIS scope ware of their obligations and subjected to supervisory measures and reporting obligations.	Notifications from Member States to the commission and ENISA	Every two years
SPO2*: Ensure that all entities that are active in sectors covered by the NIS legal framework and that are similar in size/play comparable role in the market are subject to the same regulatory regime (are either*	1. Ensure that all similar entities from sectors and services under NIS scope and of medium and large size are subject to the same NIS requirements, tested by random checks/surveys 2. Exceptions on the basis of scarce provision of	1. Random surveys/checks on a representative sample of entities per Member State and per sector/type of service confirming that similar entities (type and size)	1. Confirmed awareness and compliance check for a representative sample per Member State of entities falling under the NIS scope. 2. Minimum 4 cases per year where an entity operating in more	1. ENISA and Commission research and data based on Member States' notifications and targeted surveys 2. Cyber	Annual

Specific Objectives	*Operational objectives*	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
inside or outside the scope), no matter under which jurisdiction they fall within the EU	service or potential impact on public health and safety clearly determined and checked randomly	under the NIS scope are aware of the obligations under the NIS framework and/or subjected to supervisory measures by the competent authorities. 2. Number and type of cases where an entity operating in more than one Member State was subject to similar supervisory measures or joint supervisory action	than one Member State was subject to similar supervisory measures on all places of establishment in the EU or to joint supervisory action.	resilience business survey	
***SPO3**: Ensure that all entities that are active in sectors covered by the NIS legal framework must follow aligned obligations based on the concept of risk management when it comes to security measures and must*	1. Ensure effective compliance with security requirements, including as regards supplier relationship assessment, including via effective supervisory action. 2. Encourage/support stable investment in	1. Number and quality/weight of elements provided by the NIS framework and included in the security measures at the level of entities operating in the sectors or providing	1. Over 50% of businesses per sector/service under NIS scope respondent to the cyber resilience survey confirm an implementation of all elements provided by NIS for security measures, including	1. Cyber resilience business survey 2. Idem 3. Member States notifications to the Commission.	1-4 Annual 5 – one-off, two years since the entry into force of the new NIS legal act

Specific Objectives	*Operational objectives*	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
report incidents based on a uniform set of criteria	cybersecurity resources, including automated security tools at the level of organisations. 3. Establish/reinforce the setting at the level of competent authorities to ensure incident notification following the NIS requirements on content, format and frequency, as well as voluntary reporting of near misses and vulnerabilities. 4. Establish the notification channels and platforms for the submission of aggregated data on incidents and other notified events by the single the points of contact (SPOCs) to ENISA 5. Establish and implement policies at Member States level for supply	the services under the NIS scope. 2. ICT security investment per sector/type of service across Member States, including investment in automated security tools. 3. Number and type of incidents and other events per sector or type of service under NIS scope notified to the competent authorities and by the latter to the Commission. 4. Completeness and quality of aggregated incident-related submitted by the SPOCs to ENISA 5. Adopted policies on	supplier relationship assessment. 2. Over 60% of businesses per sector/service under NIS scope respondent to the cyber resilience survey confirm investments in automated security tools. 3. All competent authorities report significant incidents to the Commission for over half of the essential sectors and services under NIS scope. 4. Quality real-time aggregated data submitted by SPOCs of all Member States to ENISA. 5. Supply chain policies implemented in each Member State	4. SPOCs submissions to ENISA 5. Member States' notifications in the Cooperation Group and peer reviews	

Specific Objectives	*Operational objectives*	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
	chain security	supply chain security developed at Member States and modalities of implementation			
SPO4: *Ensure that competent authorities enforce the rules laid down by the legal instrument more effectively through aligned supervisory and enforcement measures*	1. Ensure alignment of minimum requirements for supervisory action by the competent authorities for essential entities and effective application thereof. 2. Provide for a minimum list of sanctions for non-compliance of essential entities with the NIS requirements and ensure effective application thereof. 3. Provide for and apply administrative fines for non-compliance with NIS requirements of essential entities with a maximum as provided by the NIS legal act.	1. Average number, average frequency, type and prioritisation criteria for supervisory actions conducted by competent authorities per Member State per sector/service under the NIS scope. 2. Average number and type of sanctions, other than administrative fines, applied across sectors by competent authorities in each Member State. 3. Number and level of administrative	1. Consistent application at Member State level of supervisory action covering all sectors/services under NIS scope based on established prioritisation and randomisation criteria. 2. Consistent application across Member States of sanctions other than administrative fines for non-compliance with NIS requirements. 3. Enforcement of significant administrative fines for the most serious	Member States notifications to the Commission or ENISA + cyber resilience business survey + results of peer-reviews.	Every two years

Specific Objectives	*Operational objectives*	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
	4. Ensure effective *ex post* supervision for important entities.	fines applied in the Member States for non-compliance and type of violation for which they were enforced. 4. Number and type of supervisory action applied to important entities from a representative sample of sectors/services under the NIS scope and their follow-up.	breaches of the NIS requirements. 4. Supervisory action applied *ex post* to a representative sample of important entities across Member States.		
SPO5: *Ensure a comparable level of resources across Member States allocated to competent authorities that would allow them to fulfil the core tasks laid out by the NIS framework*	Ensure that cybersecurity policies are prioritised at political level in each Member State and that the competent authorities, CSIRTs, SPOCs and the crisis management designated authorities have adequate technical, human and financial resources to effectively fulfil the tasks	Level of cybersecurity capabilities in each Member State reflected trough: • capacity to conduct supervisory action covering all sectors/services under the NIS scope; • provide support to	High level of capabilities in at least the points enumerated under the 'monitoring indicators'	peer-review ENISA and Commission assessments	continuous

Specific Objectives	***Operational objectives***	***Monitoring indicators***	***Expected targets***	***Source of data***	***Frequency of data gathering***
	provided by the NIS framework	businesses on cybersecurity measures and policies; • enforce sanctions in case of non-compliance; • develop effective and innovative policies in areas like supply chain security and coordinated vulnerability disclosure; • investment in R&D; • proactive participation in operational cooperation with other Member States, such as mutual assistance mechanisms, public private partnerships, participation in the			

Specific Objectives	***Operational objectives***	***Monitoring indicators***	***Expected targets***	***Source of data***	***Frequency of data gathering***
		CSIRTs network, etc.			
SPO6*: Ensure that essential information is exchanged between Member States by introducing clear obligations for competent authorities to share information and cooperate when it comes to cyber threats and incidents and by developing a Union joint operational crisis response capacity*	1. Ensure effective operational exchanges among Member States' authorities. 2. Ensure the setting up of coordinated vulnerability disclosure policies across Member States 3. Incentivise the setting up of sector-specific and cross-sector ISACs with public authorities participation and other public private partnerships 4. Set up a crisis management framework at national and EU levels and institutionalising of EU-CyCLONe	1. Number of instances when the mutual assistance mechanism was triggered in cross-border cases and number of joint supervision actions. 2. Number of coordinated vulnerability disclosure policies set up at the level of Member States, number of national CSIRTs designated as coordinators/ facilitators + number of discovered vulnerabilities notified to ENISA. 3. Number of operational ISACs and their outcomes; number of other	1. Mutual assistance mechanism applied in a relevant number of cases and use of joint supervisory action. 2. Coordinated vulnerability disclosure policies set up in all Member States, responsible CSIRTs designated and vulnerabilities discovered notified to ENISA. 3. Steady increase across all Member States in number of sector-specific and cross-sector ISACs and other public-private partnerships. 4. Crisis management frameworks in lace at national level and CyCLONe and	Submissions of Member States and peer-review ENISA and Commission assessments	1. Annual 2. One-off: two years after the entry into force of new NIS framework for setting the policies and designation of CSIRT and annual monitoring of notifications of vulnerabilities discovered. 3. Every two years 4. One-off for the setting up of the frameworks: two years after the entry into force of the new NIS legal act and

Specific Objectives	*Operational objectives*	*Monitoring indicators*	*Expected targets*	*Source of data*	*Frequency of data gathering*
		public private partnerships. 4. Number of national authorities designated and procedures in place for crisis management national framework + extent of participation in CyCLONe	dedicated Cooperation Group fully functional.		continuous monitoring of operationally.