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)

European Commission
Directorate-General for Communications Networks, Content and Technology
Unit H2 – Cybersecurity and Digital Privacy Policy

Closing Workshop – 12th and 13th October 2020

This work is carried out by

Disclaimer

Overview of the targeted consultations

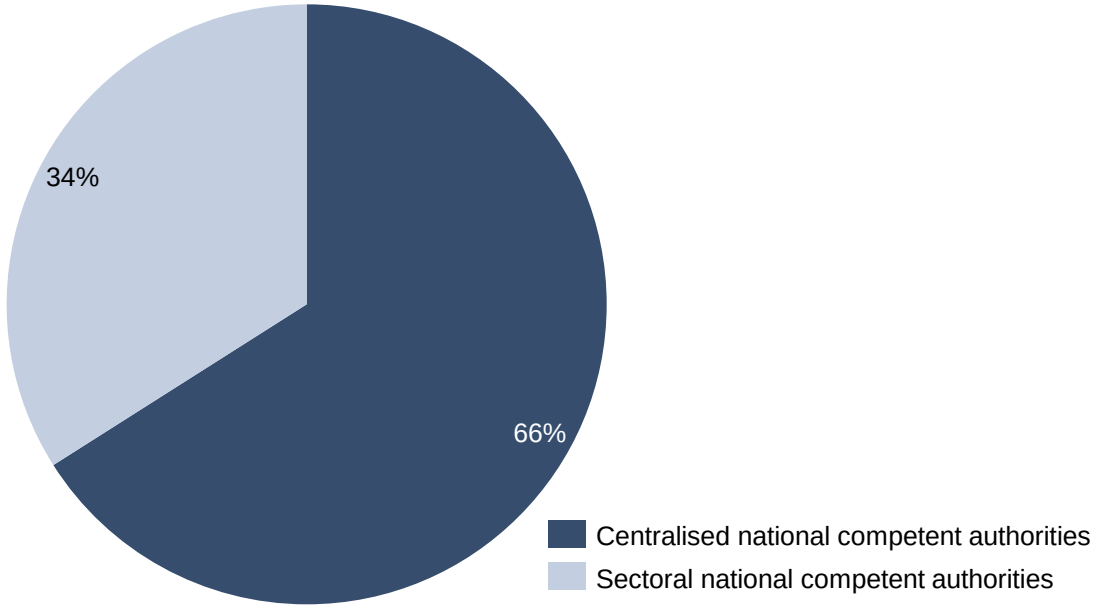
Targeted consultations – Online Surveys

	Online Surveys
Which stakeholder groups were consulted?	• **National Competent Authorities** (CAs, CSIRTs and SPOCs). • **Operators of Essential Services** (OESs). • **Digital Service Providers** (DSPs).
How many Online Surveys?	**3 questionnaires** were available online for all stakeholder groups: • **CAs** with **46** respondents. • **OESs** with **49** respondents. • **DSPs** with **9** respondents.
When were the Online Surveys delivered?	The **launch date** was the week of **13 – 17 July**. The Online Surveys were **closed on 4 September**.

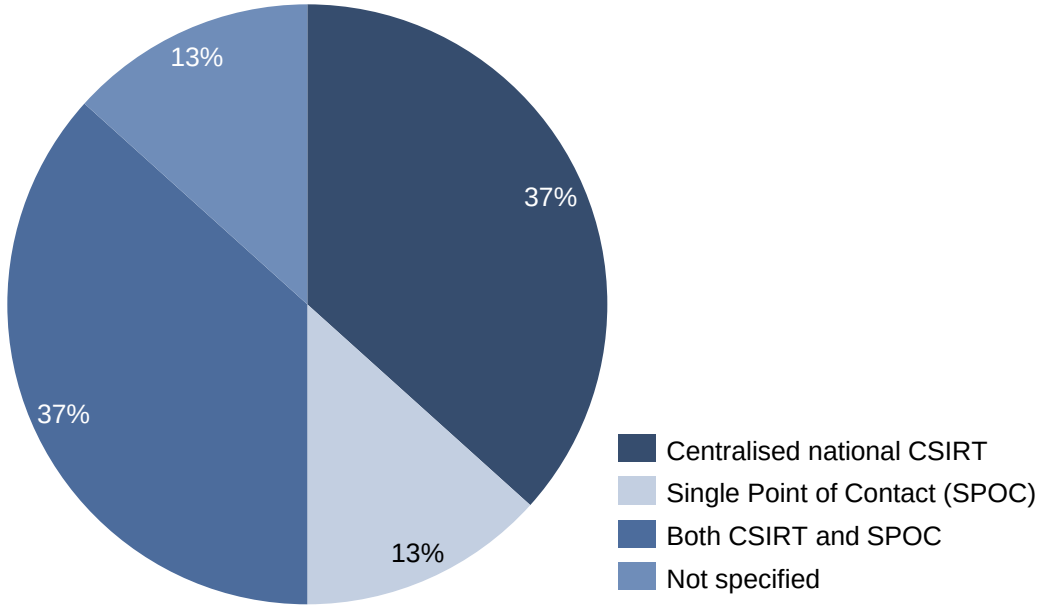
Online Surveys – CAs profile

CAs respondents were asked '**In which capacity are you replying to this questionnaire?'.**

The pie chart below **shows the distribution of respondents to the CAs online survey** given the following categories: (1) Centralised national competent authority; (2) Sectoral national competent authority.



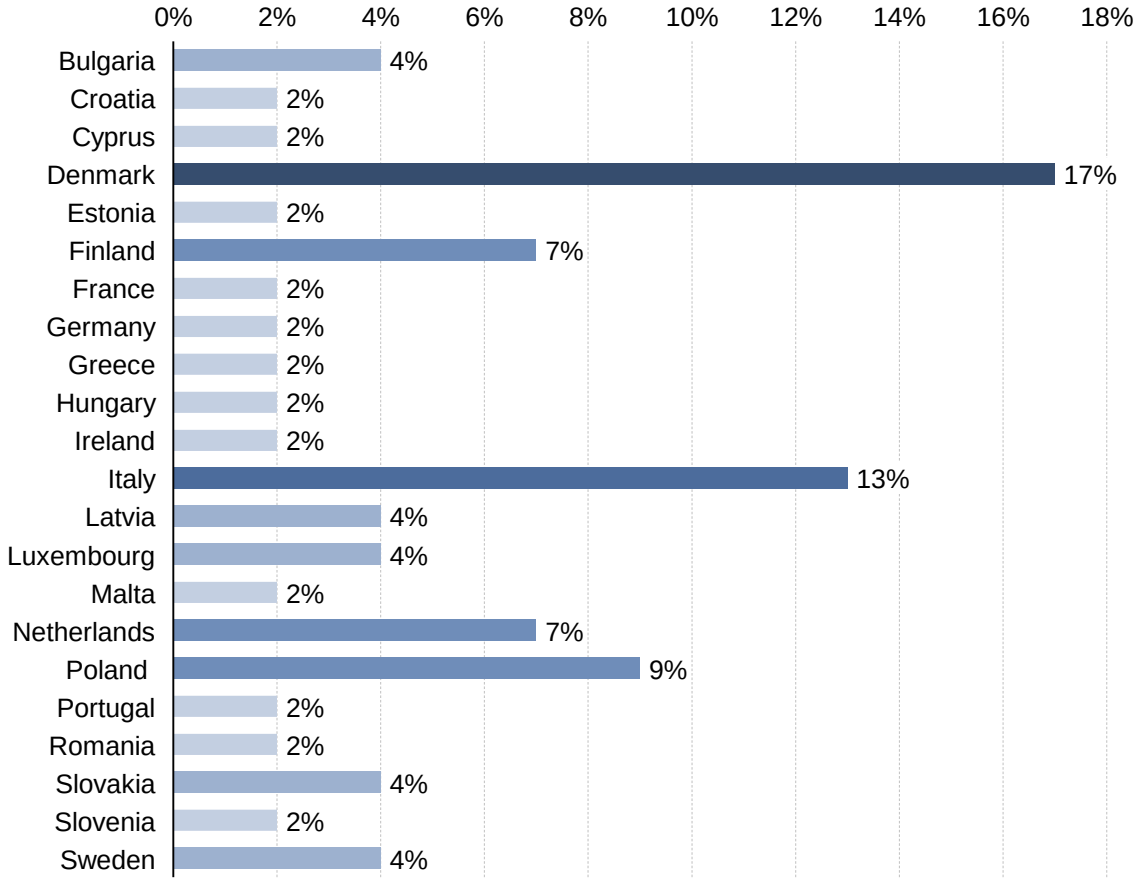
The pie chart below **illustrates the sub-division of the Centralised national competent authority** into (1) Centralised national CSIRT; (2) Single Point of Contact; (3) Both SPOC and CSIRT; (4) Not specified centralised national competent authority.



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46

Online Surveys – CAs countries of origin

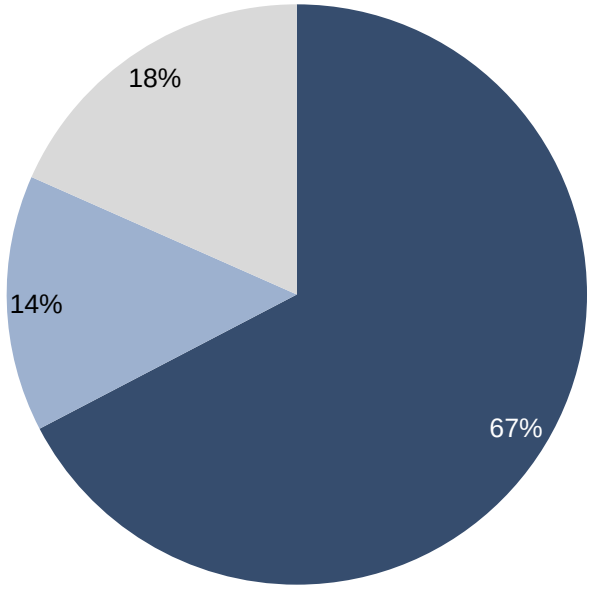
The histogram below shows the countries of origin of the consulted CAs.



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46

Online Surveys – OESs profile

OESs respondents were asked **'In which capacity are you replying to this questionnaire?'** and given the following options: (1) Operator of Essential Services (OES) covered within the NIS Directive; (2) Entities providing services outside the current scope of the NIS Directive which are essential to the functioning of the economy and society such as telecoms, public administration, chemical and food sector, social platforms, media, etc.; (3) Other. The pie chart below shows the distribution of respondents to the OESs online survey:



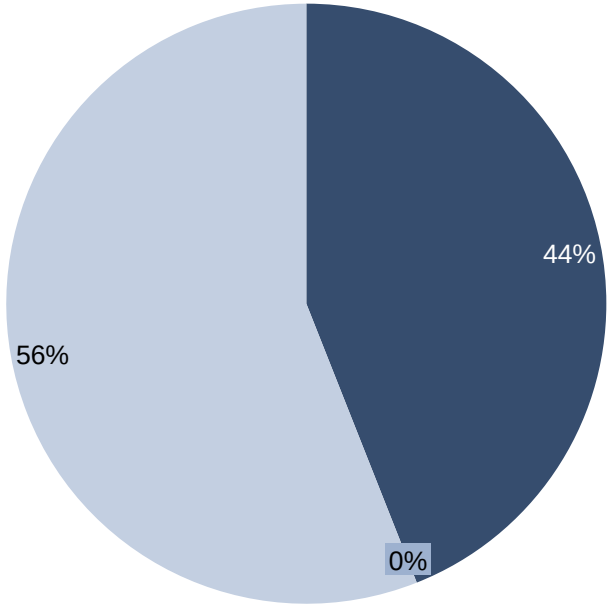
- Operator of essential services (OES) covered within the NIS Directive
- Providers of essential services which are outside the current scope of the Directive
- Other

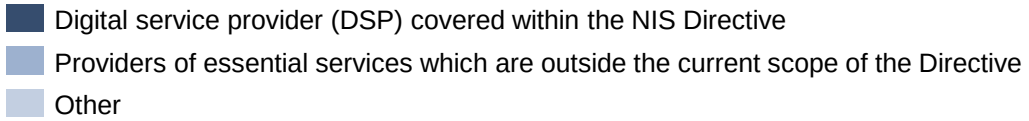
Other:	
	Financial sector collaborative defence and information sharing consortium
	ATM/ANS
	DSP
	Cybersecurity researcher
	EU Agency (Energy Sector)
	Trade association
	Telecoms
	Professional association
	German Technical and Scientific Association for Gas and Water

Source: Targeted online survey conducted by Wavestone with OESs. N for OESs=49

Online Surveys – DSPs profile

DSPs respondents were asked **'In which capacity are you replying to this questionnaire?'** and given the following options: (1) Digital Service Provider (DSP) covered within the NIS Directive; (2) Entities providing services outside the current scope of the NIS Directive which are essential to the functioning of the economy and society such geolocation services, social network and data centres and content delivery networks; (3) Other. The pie chart below shows the distribution of respondents to the DSPs online survey.





Other:

Providers of secure hardware for OES and DSPs
Information security company
Interested party
Cybersecurity Company
Provider of security technologies

Source: Targeted online survey conducted by Wavestone with DSPs. N for DSPs=9

Targeted consultations – In-depth interviews

	In-depth interviews
Which stakeholder groups were consulted?	• **National Competent Authorities** (CAs). • **Operators of Essential Services** (OESs). • **Digital Service Providers** (DSPs). • **EU Institutions and Agencies**. • **Think-Tanks**.
How many interviews were conducted?	**16 interviews**: 4 CAs; 7 OESs; 2 DSPs; 2 EU Institutions and Agencies; 1 Think-Tank.
When were the in-depth interviews delivered?	The in-depth interviews were conducted from **second half of July to the first week of September (23 July 2020 – 8 September 2020**.

Main findings from the targeted consultations

Limitations of the targeted consultations

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

- **The lack of available evidences in some cases prevented a quantitative analysis** of the changes introduced by the NIS Directive, e.g. costs and benefits of implementing the NIS Directive;
- The partial contributions to the online surveys by the Member States (**responses covered 22 EU countries**) prevented a fully-fledged comparative analysis across the European Union;
- **The low response rate from DSPs** in all consultation activities carried out by the study, which may result from the “light touch approach”, ex-post supervision towards DSPs, and compliance to several international standards; and
- **The limited evidences on the actual impacts of the Directive**, since the Directive has been implemented by the Member States only as of 2018.

The above-mentioned issues limited the analysis especially in relation to the **“EU added-value”, “effectiveness” and “efficiency” evaluation criteria**.

Relevance

The relevance analysis assessed how the objectives set at the time of the NIS Directive adoption correspond to the (current) needs and problems in society and the economy, as well as to the wider EU policy priorities and goals.

The problems and needs that were considered most prominent when the NIS Directive was adopted **are still relevant** and most likely require action at EU level.

Main problems:

- 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.

Main needs:

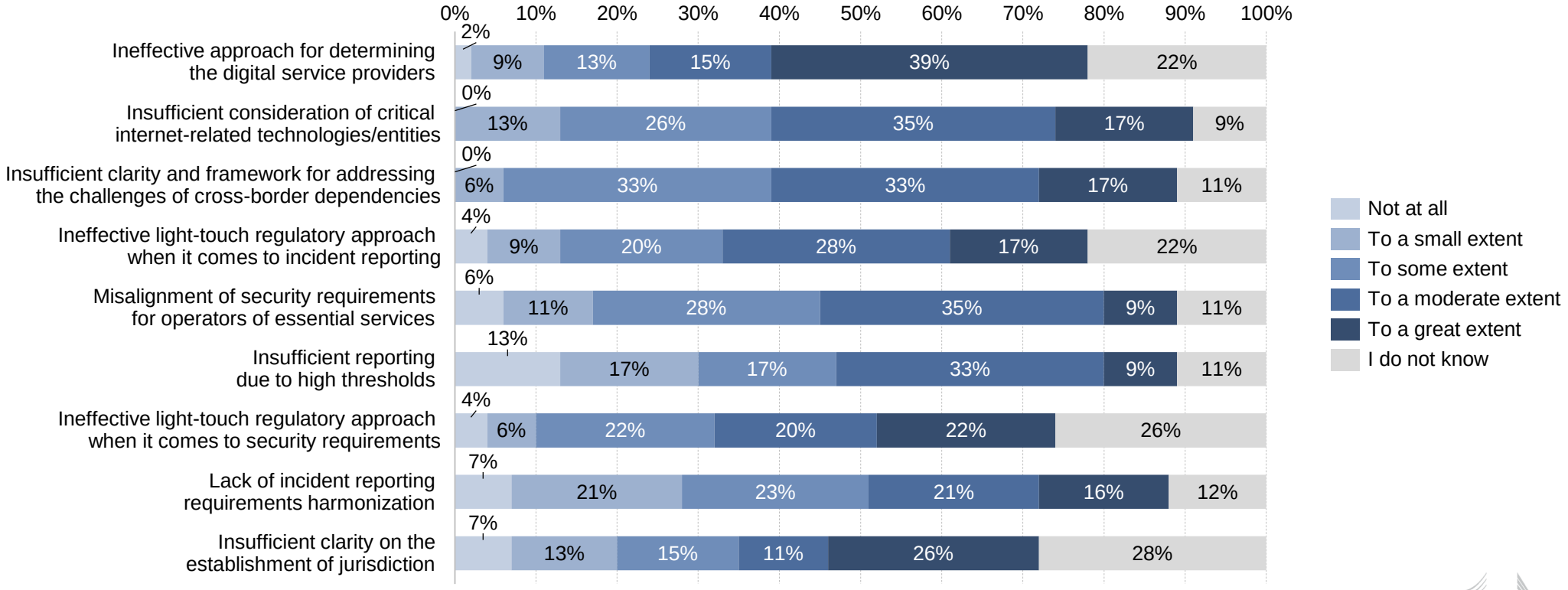
- to implement security measures to manage cybersecurity risks, and prevent, minimise and notify incidents;
- to harmonise the identification process of OESs across the Member States; and
- to addresss the ineffective approach for determining the DSPs falling under the scope of the Directive.

New challenges:

- the increasing interconnectedness and reliance on digital infrastructures, technologies and online systems; and
- the resilience and trust in the supply chain.

Relevance – NISD shortcomings - CAs

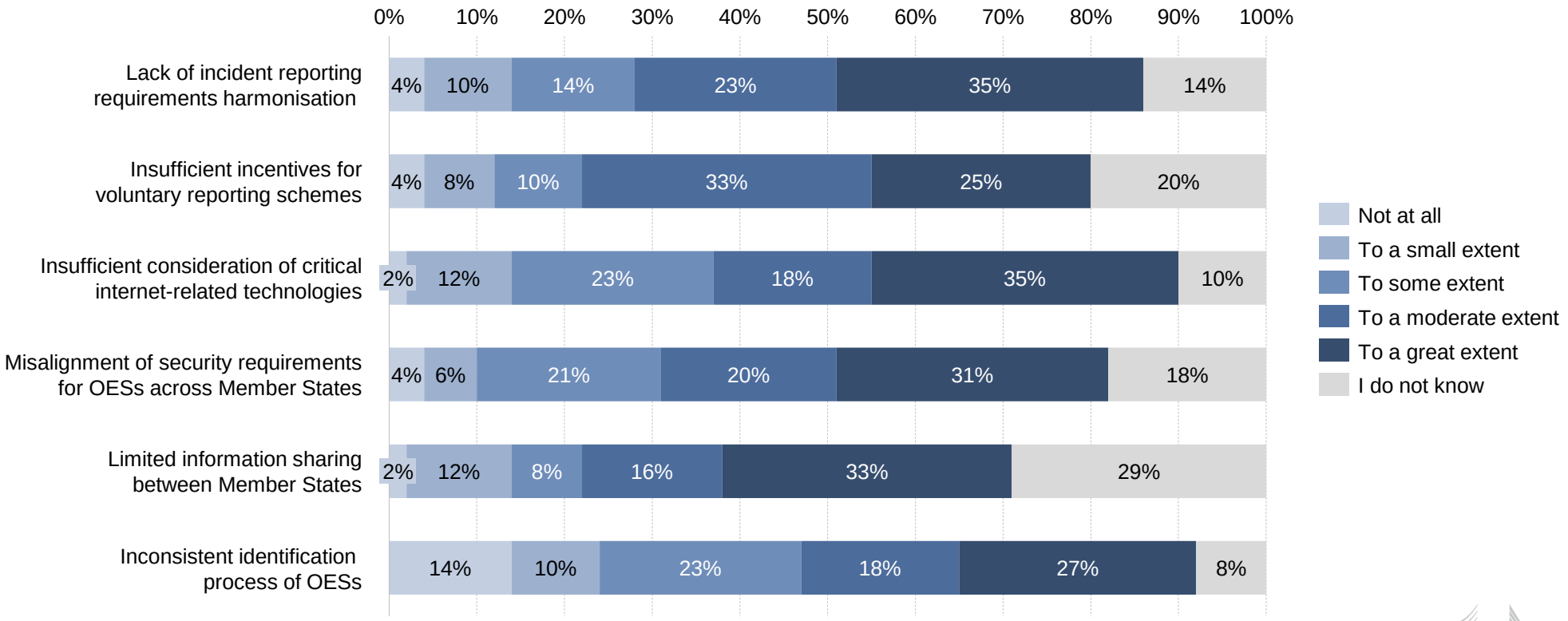
CAs respondents were asked **'Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive?'.** The histogram below shows the distribution of responses to the CAs online survey:



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46

Relevance – NISD shortcomings - OESs

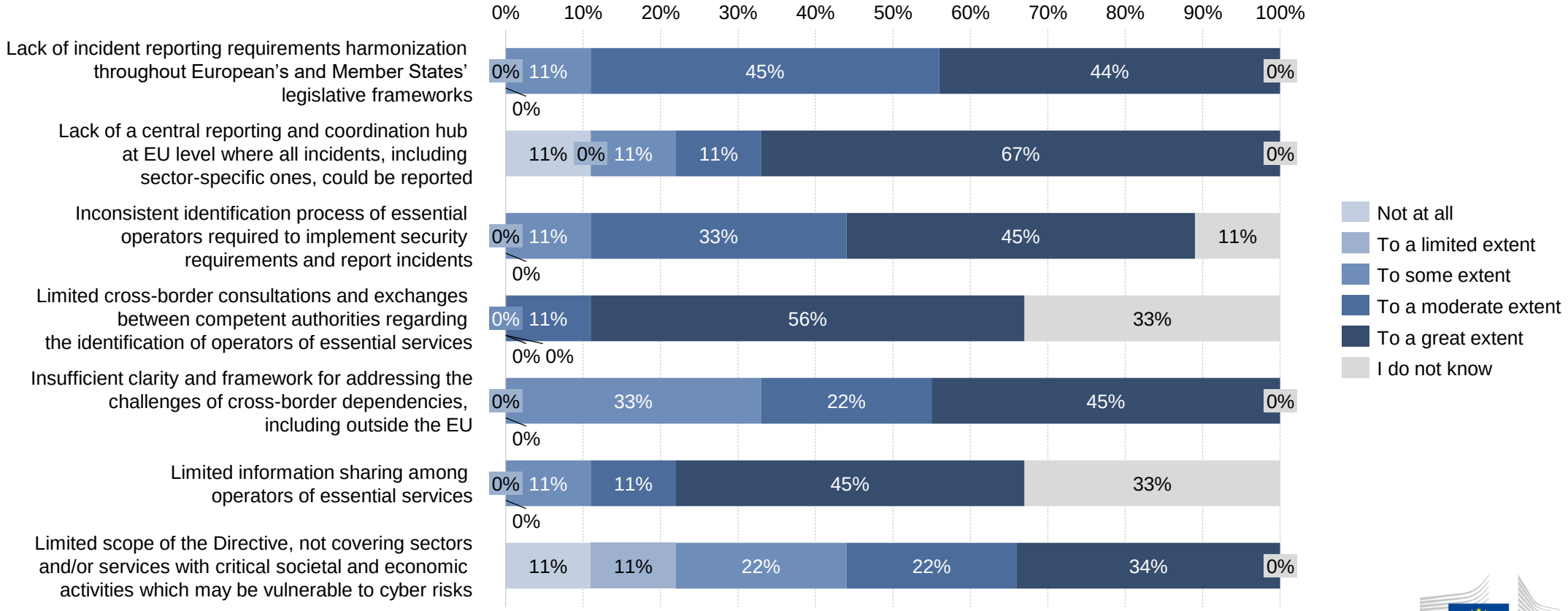
OESs respondents were asked **'Taking account of the potential problems that need to be addressed today with cybersecurity legislation at EU level, to what extent do the following issues represent shortcomings of the NIS Directive?'.** The histogram below shows the distribution of responses to the OESs online survey:



Source: Targeted online survey conducted by Wavestone with OESs. N for OESs=49

Relevance – NISD shortcomings - DSPs

DSPs respondents were asked **'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?'.** The histogram below shows the distribution of responses to the DSPs online survey:



Source: Targeted online survey conducted by Wavestone with DSPs. N for DSPs=9

Coherence

The analysis of the coherence criterion focuses on the legal examination of concepts and definitions, as well as specific provisions of other EU interventions, with a view to assess their consistency with the NIS Directive.

The legislation examined include but are not limited to: 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**).

External coherence

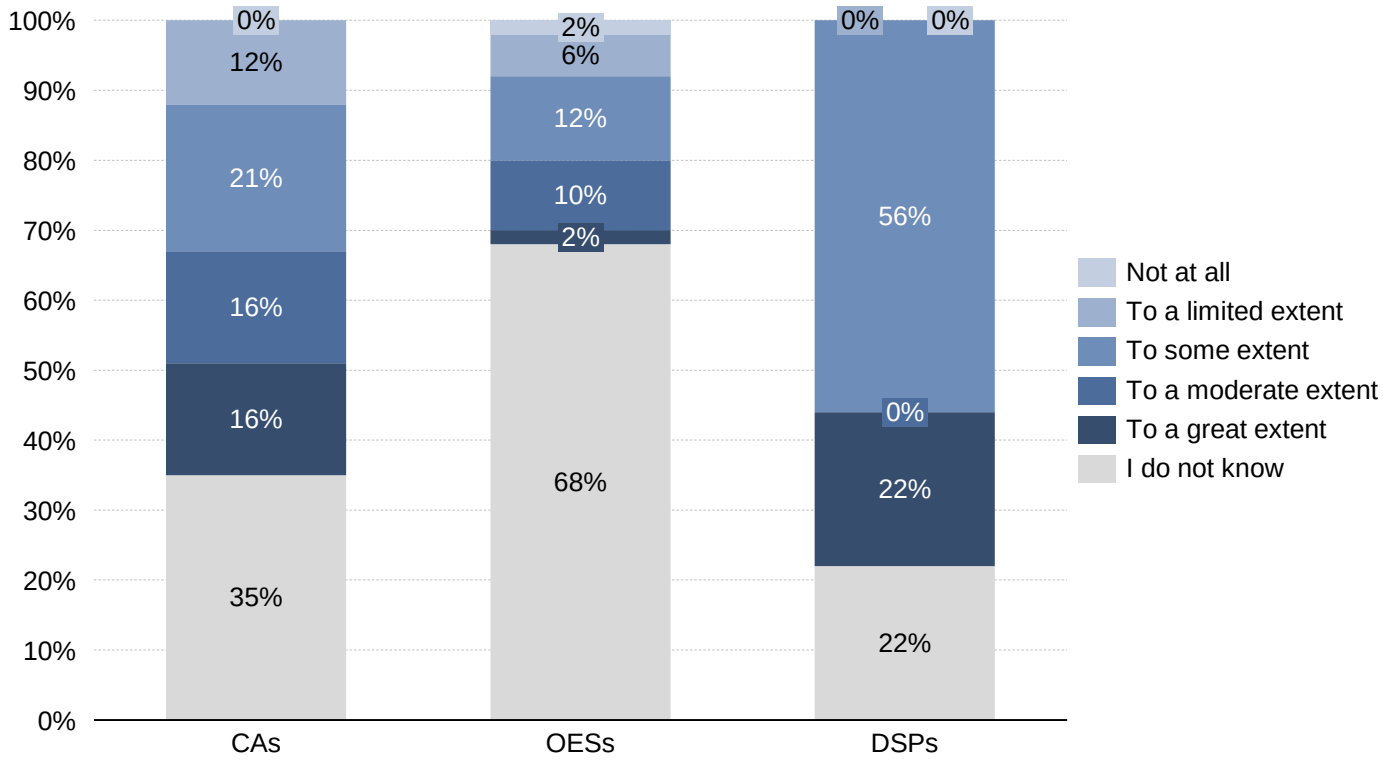
There is a good degree of consistency of concepts and definitions between the Directive and the other EU instruments. However, **a better alignment among certain legal instruments could still be reached in relation to definitions**, such as the notion of 'incident', **as well as reporting requirements**, which are heterogeneous in terms of reporting authorities, thresholds, timeframe, and penalties.

Internal coherence

Although the majority of the respondents declared that the definitions provided in the NIS Directive are clear enough, **a number of undefined legal concepts are present in the Directive**, e.g. definition of OESs and DSPs; 'significant' or 'substantial' impact and 'appropriate and proportionated technical and organisational measures to manage the risks'.

External Coherence - EECC

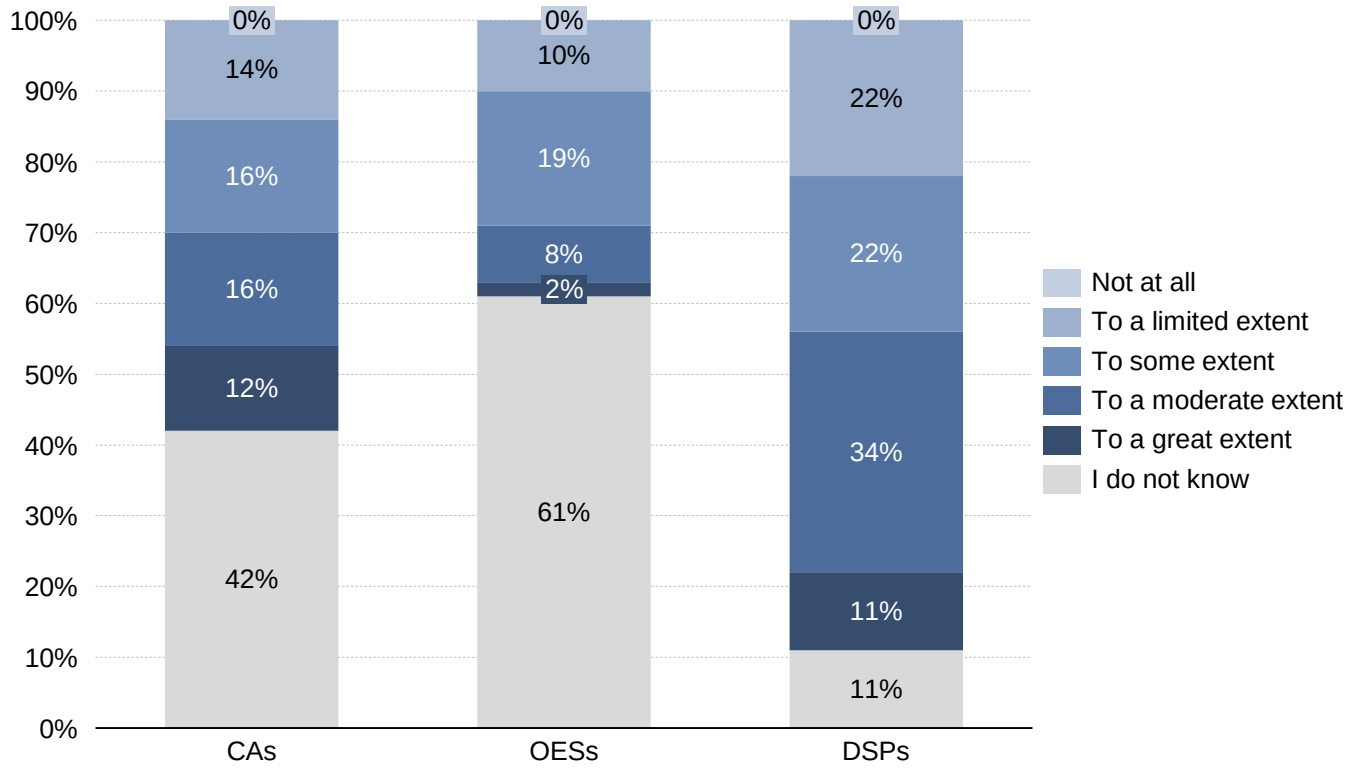
CAs, OESs, and DSPs respondents were asked **'To what extent do you believe that the provisions of the NIS Directive and obligations stemming from these provisions are coherent with the following EU initiatives?'.** The histogram below shows the distribution of responses to the online survey:



Source: Targeted online survey conducted by Wavestone with CAs, OESs, and DSPs. N for CAs=43; N for OESs= 49; N for DSPs= 9.

External Coherence - eIDAS

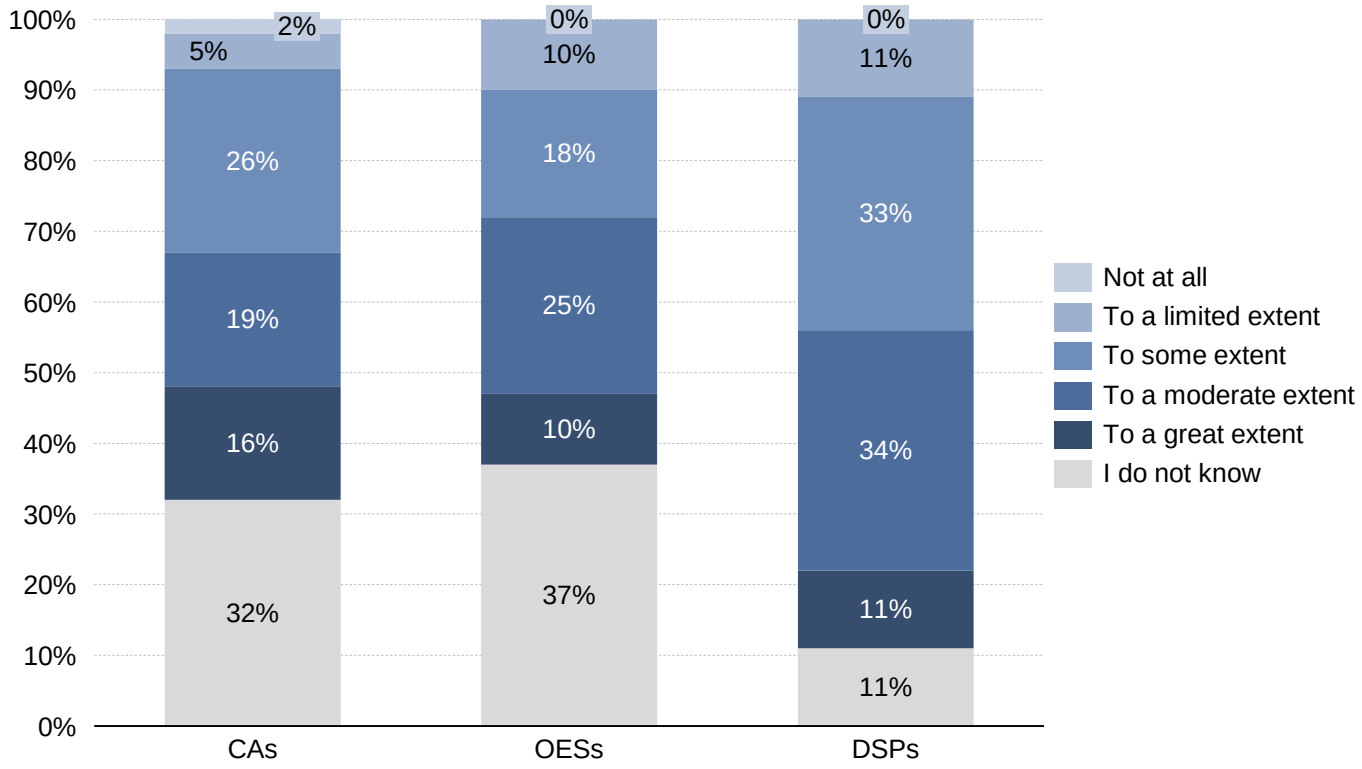
CAs, OESs, and DSPs respondents were asked **'To what extent do you believe that the provisions of the NIS Directive and obligations stemming from these provisions are coherent with the following EU initiatives?'.** The histogram below shows the distribution of responses to the online survey:



Source: Targeted online survey conducted by Wavestone with CAs, OESs, and DSPs. N for CAs=43; N for OESs= 49; N for DSPs= 9.

External Coherence - GDPR

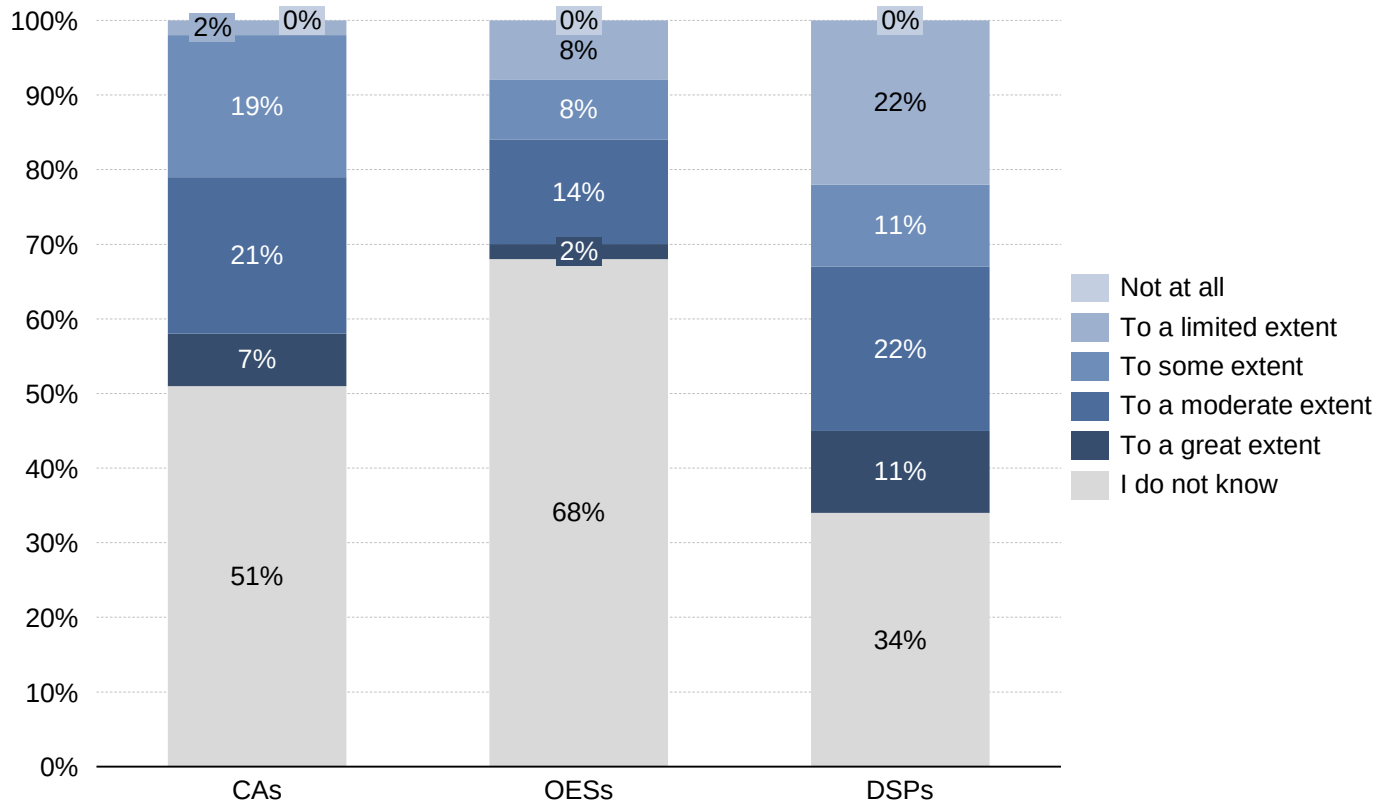
CAs, OESs, and DSPs respondents were asked **'To what extent do you believe that the provisions of the NIS Directive and obligations stemming from these provisions are coherent with the following EU initiatives?'.** The histogram below shows the distribution of responses to the online survey:



Source: Targeted online survey conducted by Wavestone with CAs, OESs, and DSPs. N for CAs=43; N for OESs= 49; N for DSPs= 9.

External Coherence - PSD2

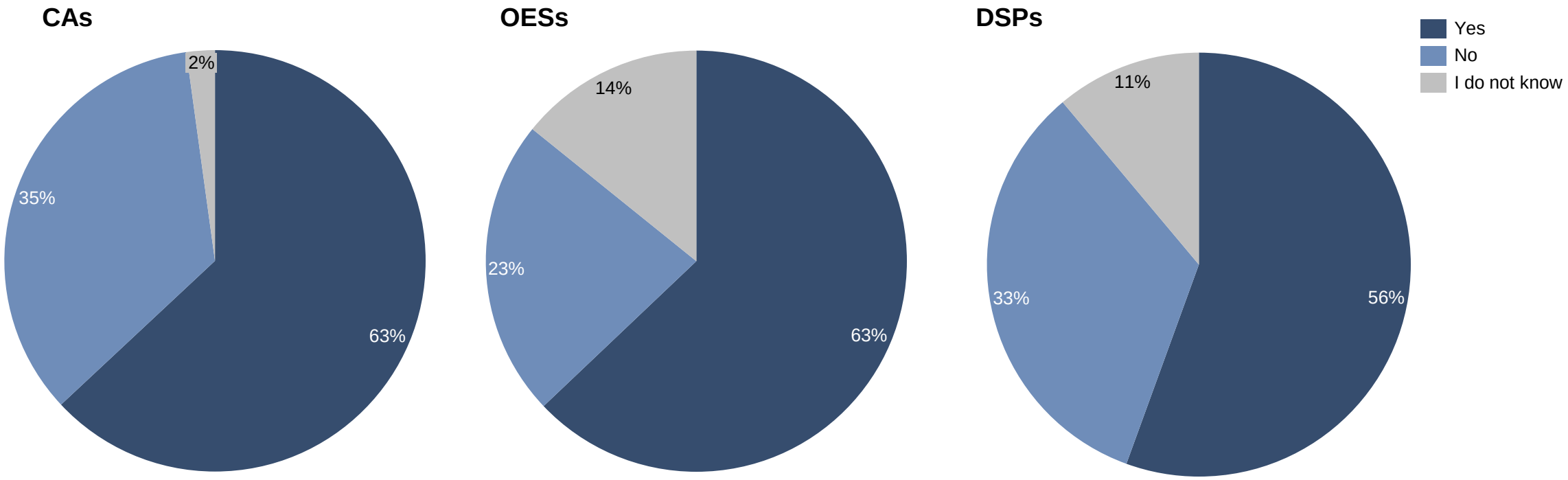
CAs, OESs, and DSPs respondents were asked **'To what extent do you believe that the provisions of the NIS Directive and obligations stemming from these provisions are coherent with the following EU initiatives?'.** The histogram below shows the distribution of responses to the online survey:



Source: Targeted online survey conducted by Wavestone with CAs, OESs, and DSPs. N for CAs=43; N for OESs= 49; N for DSPs= 9.

Internal Coherence – CAs, OESs and DSPs

CAs, OESs and DSPs respondents were asked **'In your view, are the definitions and/or concepts provided in the Directive clear enough?'.**
The pie charts below shows the distribution of responses to the CAs, OESs and DSPs online surveys:



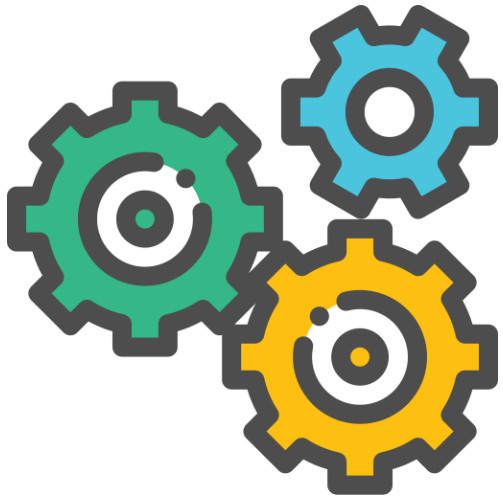
Source: Targeted online survey conducted by Wavestone with CAs, OESs and DSPs. N for CAs=46; N for OESs=49; N for DSPs=9

EU Added Value

The EU added value criterion investigates the extent to which the NIS Directive has contributed to boost the overall level of cybersecurity in the EU in a way that could not have been achieved by Member States on their own, as well as it examines the need for continued EU action.

The NIS Directive:

- created a **common legal framework to ensure a high level of network and information security** across the Union;
- ensured the implementation of a **minimum set of security requirements;**
- promoted the adoption of **national frameworks and the designation of national competent authorities** in charge of the monitoring and implementation of the Directive;
- **raised awareness about the importance of cybersecurity** in the EU; and
- fostered **cooperation and exchange of information** at the EU level.

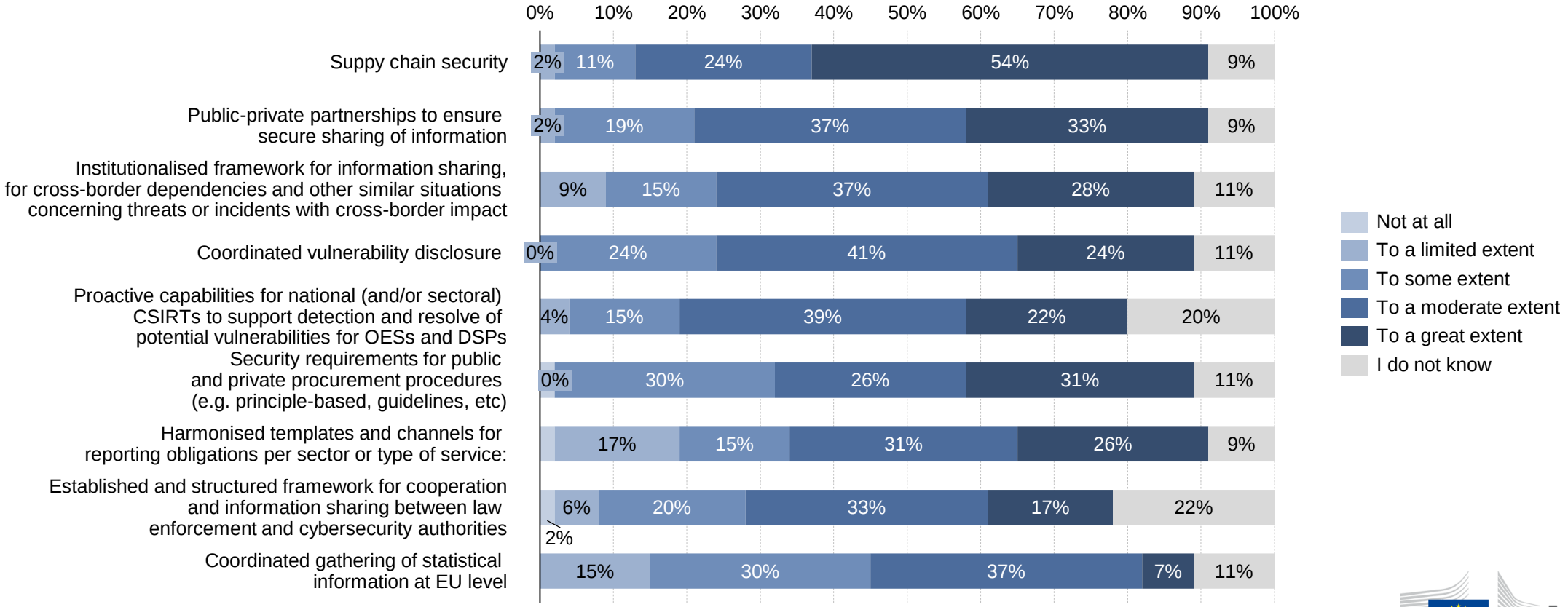


Several elements suggest that EU intervention is still needed:

- the **general objective of the Directive has not been fully achieved**;
- **harmonisation between Member States**, despite significative efforts, **remains incomplete**, e.g. OESs identification;
- **new policy measures should be considered** within the revision of the NIS Directive, e.g. supply chain security, new technologies, public-private partnerships.

EU Added Value – New policy measures - CAs

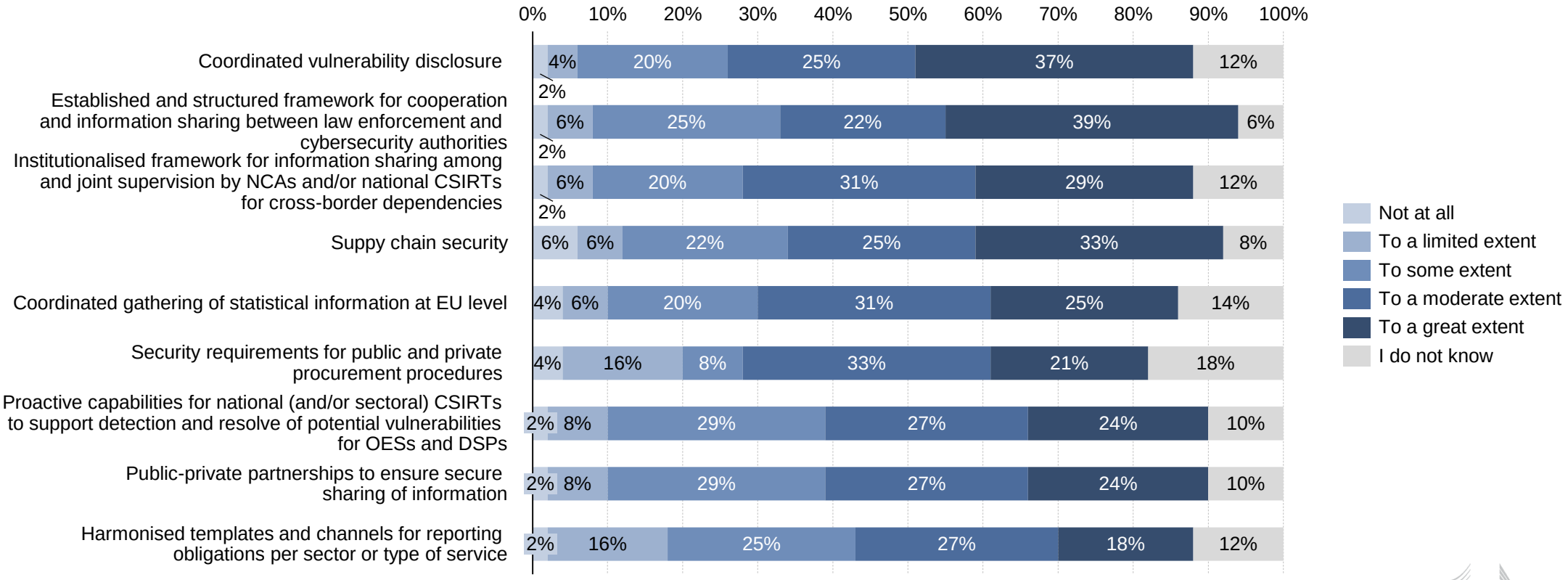
CAs respondents were asked **'In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered?'.** The histogram below shows the distribution of responses to the CAs online survey:



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46

EU Added Value – New policy measures - OESs

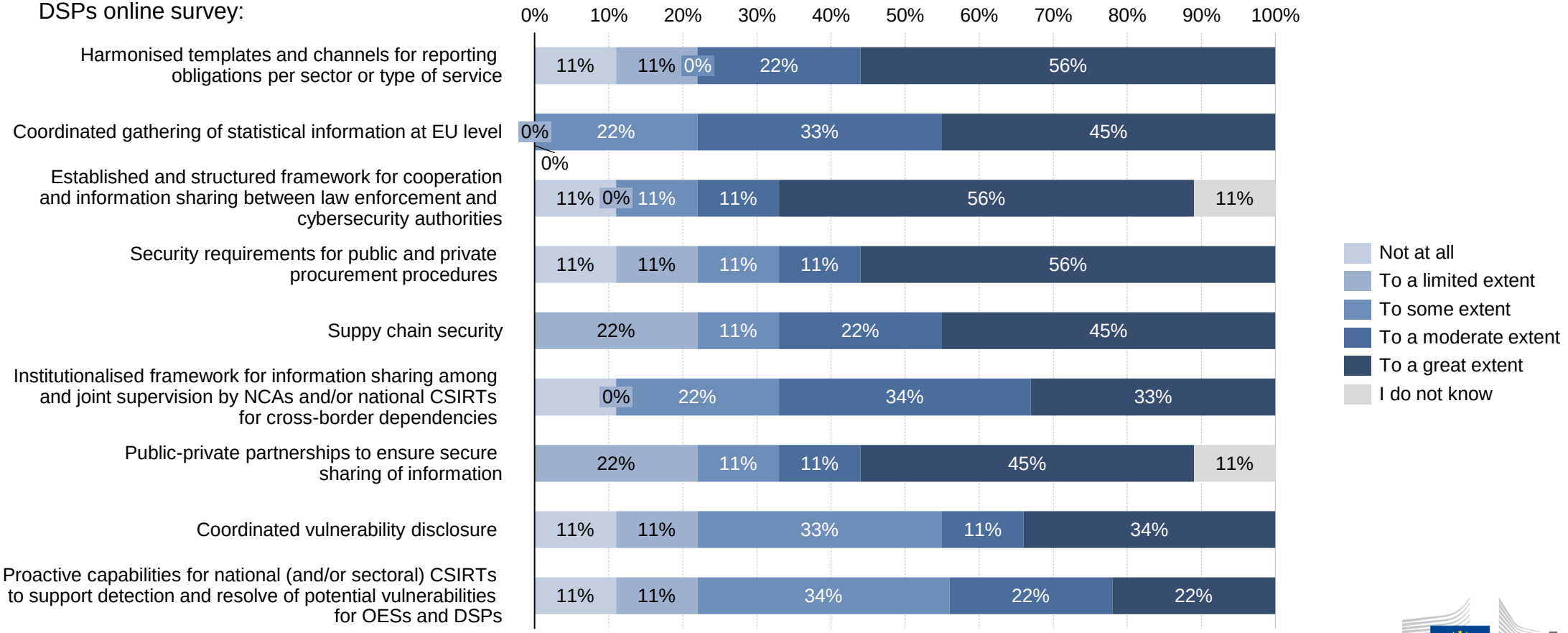
OESs respondents were asked **'In light of a potential revision of the NIS Directive, to what extent should the following new policy concepts, currently under discussion throughout the review process, be considered?'.** The histogram below shows the distribution of responses to the OESs online survey:



Source: Targeted online survey conducted by Wavestone with OESs. N for OESs=49

EU Added Value – New policy measures - DSPs

DSPs respondents were asked **'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?'.** The histogram below shows the distribution of responses to the DSPs online survey:



Source: Targeted online survey conducted by Wavestone with DSPs. N for DSPs=9

Effectiveness

Effectiveness assessed the extent to which the general and specific objectives of the NIS Directive have been achieved.

General objective

The NIS Directive contributed to achieve a high common level of security of network and information systems within the Union to improve the functioning of the internal market.

Specific objectives:

(i) Setting out of national frameworks

All Member States have a national cybersecurity strategy in place and competent authorities in charge of the implementation of the Directive.

There is need for improvement concerning:

- public-private partnerships;
- incentives for the private sector to invest in security measures; and
- the implementation of risk assessment procedures.

(ii) Security requirements/incident notifications for OESs & DSPs

OESs and DSPs effectively manage risks posed to the security of network and information systems.

There is 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.

(iii) Cooperation at EU level

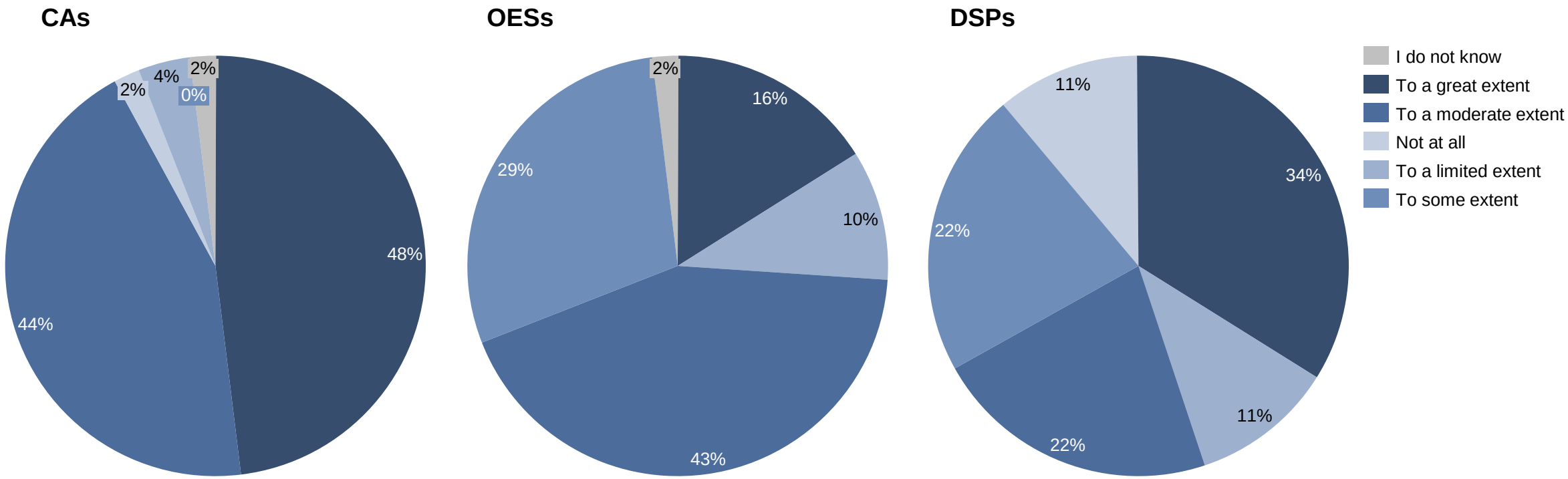
The **Cooperation Group** was effective in assisting Member States in building capacity and exchanging best practices and experiences.

The **CSIRTs Network** had a positive impact in clarifying actors' role and responsibilities within the incident response process.

There is need for improvement concerning the communication and collaboration between these two entities.

Effectiveness

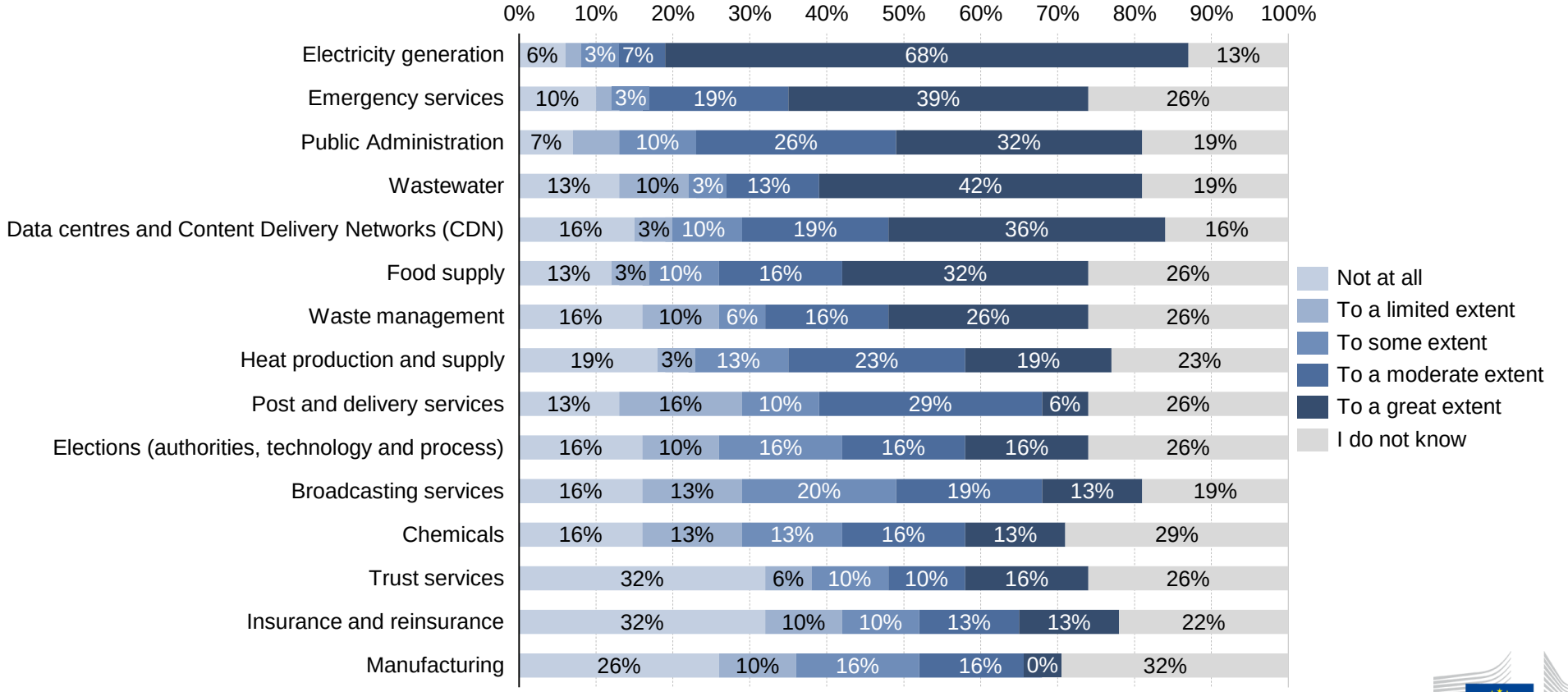
CAs, OESs, and DSPs respondents were asked **'In your opinion, to what extent were the overall provisions laid down in the NIS Directive effective for achieving its general objective (i.e. a high common level of security)?'.** The histogram below shows the distribution of responses to the CAs, OESs, and DSPs online surveys:



Source: Targeted online survey conducted by Wavestone with CAs, OESs and DSPs. N for CAs=46; N for OESs=49; N for DSPs=9

Effectiveness – Additional sectors - CAs

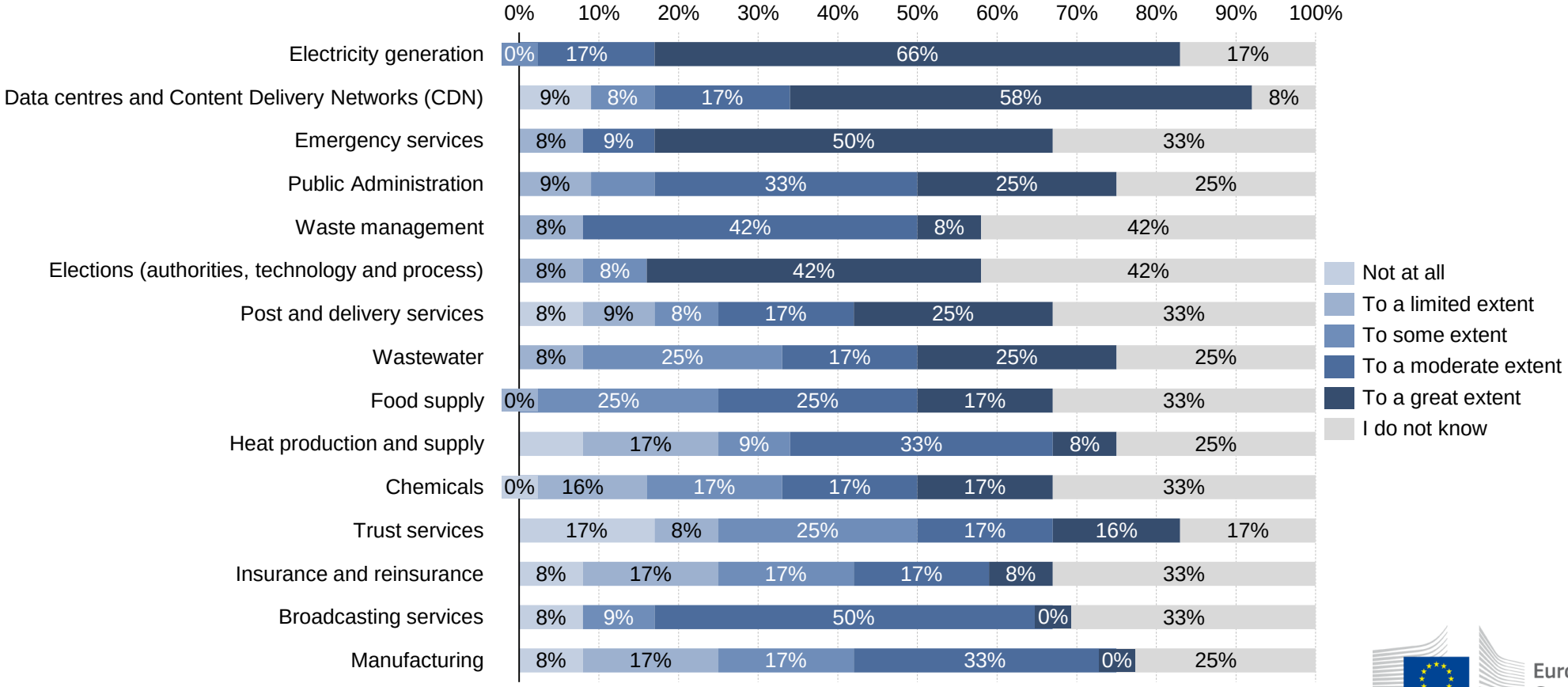
CAs respondents were asked **'In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile?'.** The histogram below shows the distribution of responses to the CAs online surveys:



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46

Effectiveness – Additional sectors - OESs

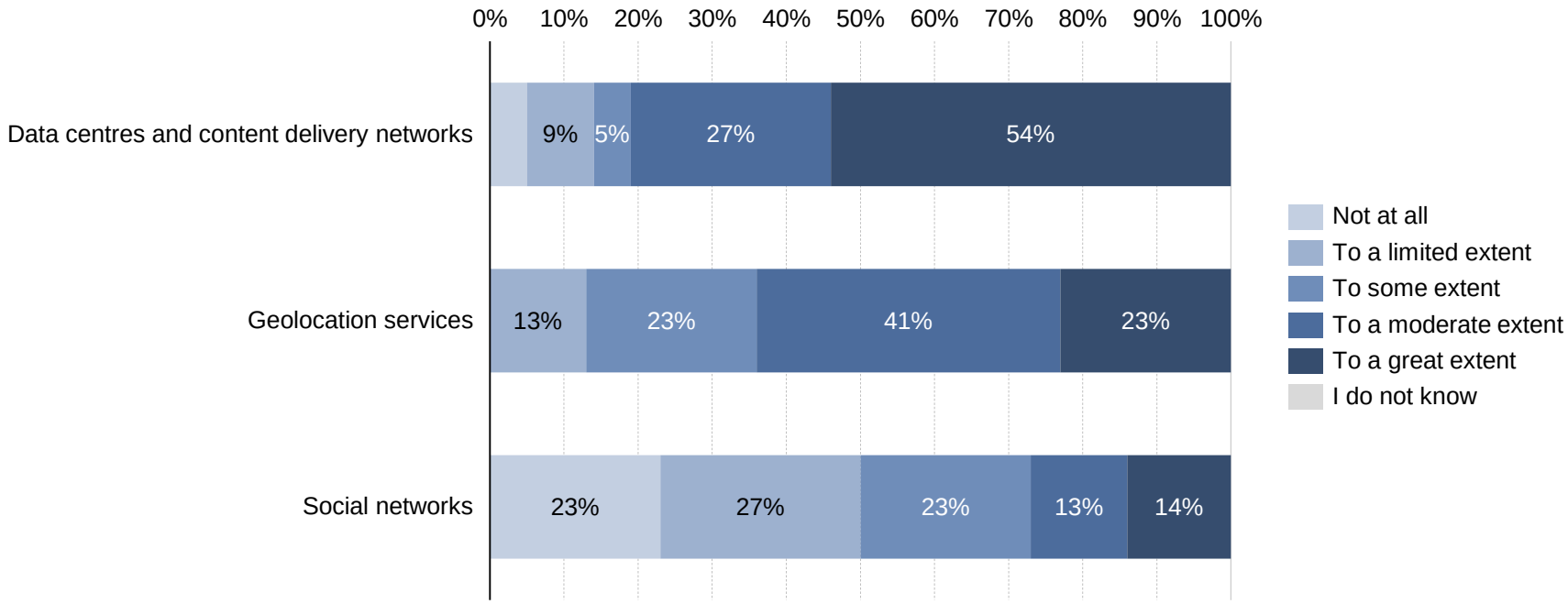
OESs respondents were asked **'In your opinion, to what extent should the below sectors, currently not in the scope of the Directive, be considered to be included within a potentially expanded scope of the Directive, given their cybersecurity related risk profile?'.** The histogram below shows the distribution of responses to the OESs online surveys:



Source: Targeted online survey conducted by Wavestone with OESs. N for OESs=49

Effectiveness – Additional types of DSPs - CAs

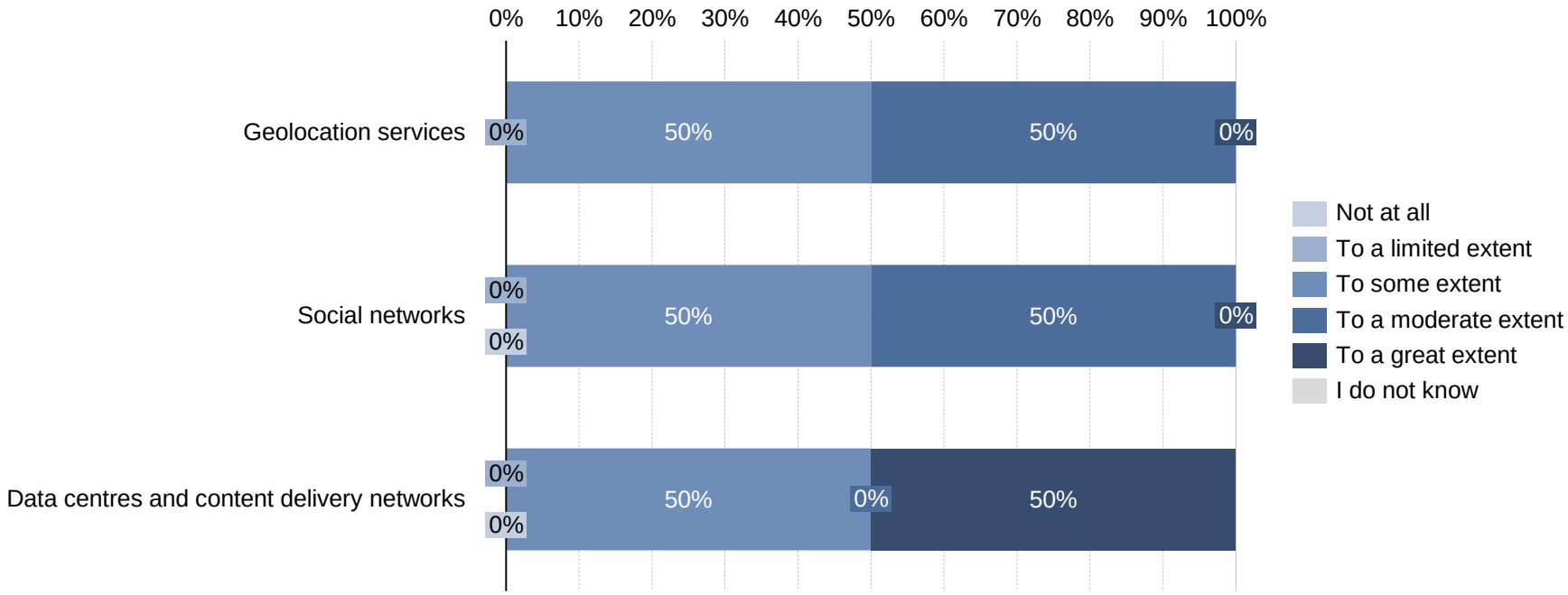
CAs respondents were asked **'In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity-related risk profile?'.** The histogram below shows the distribution of responses to the CAs online surveys:



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46

Effectiveness – Additional types of DSPs - DSPs

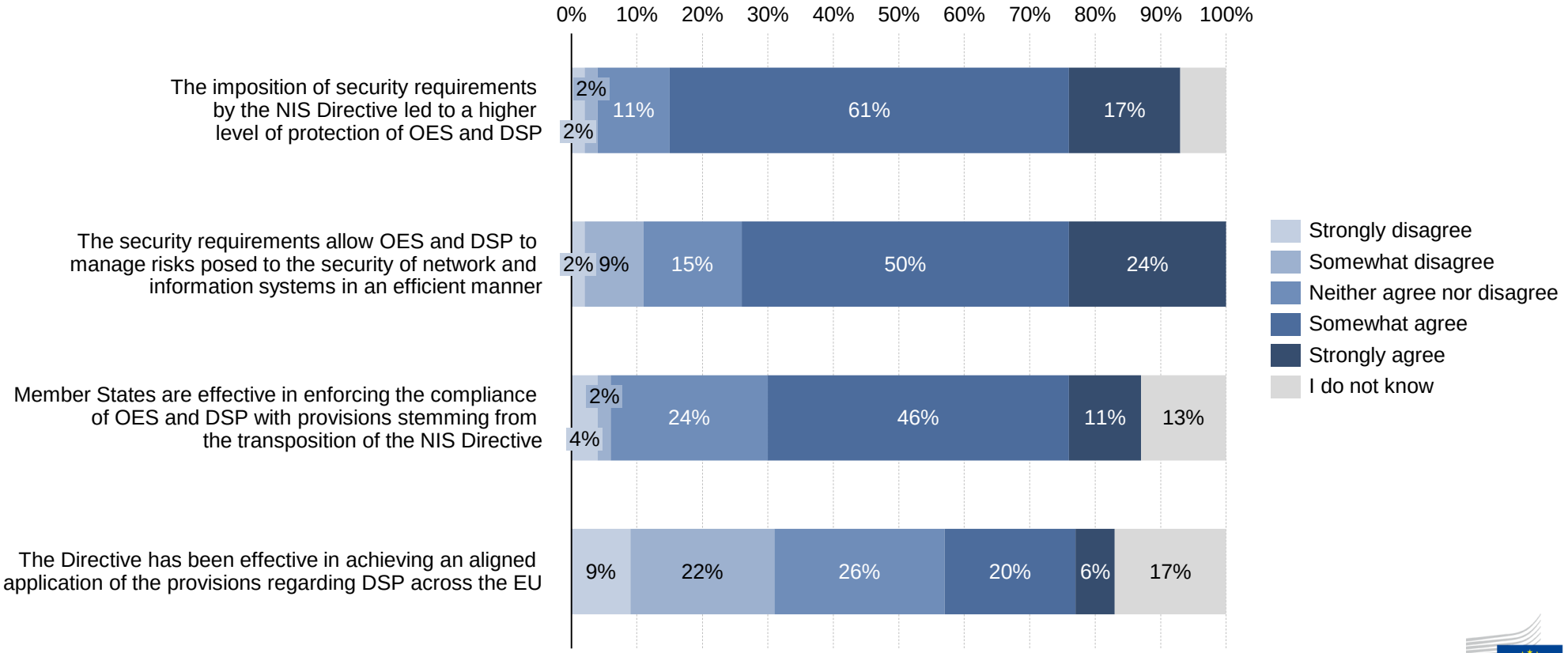
DSPs respondents were asked **'In your opinion, to what extent should the below types of digital service providers, currently not in the scope of the Directive, be considered as part of Annex III given their cybersecurity-related risk profile?'.** The histogram below shows the distribution of responses to the DSPs online surveys:



Source: Targeted online survey conducted by Wavestone with DSPs. N for DSPs=9

Effectiveness – Security requirements and incident notification - CAs

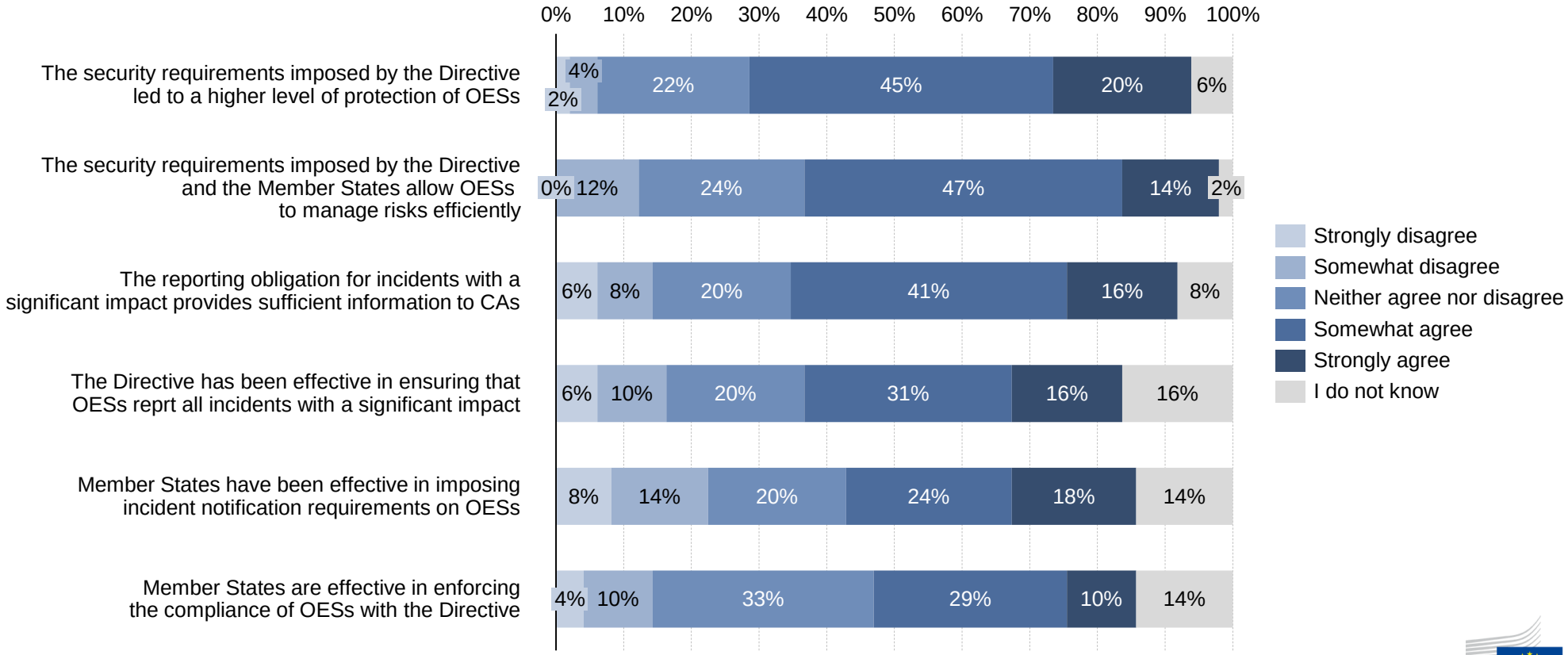
CAs respondents were asked **'Thinking about the security requirements and the incident notification provisions laid down in Article 14 and 16 of the Directive, and according your experience, to what extent would you agree with the following statements?'.** The histogram below shows the distribution of responses to the CAs online surveys:



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46

Effectiveness – Security requirements and incident notification - OESs

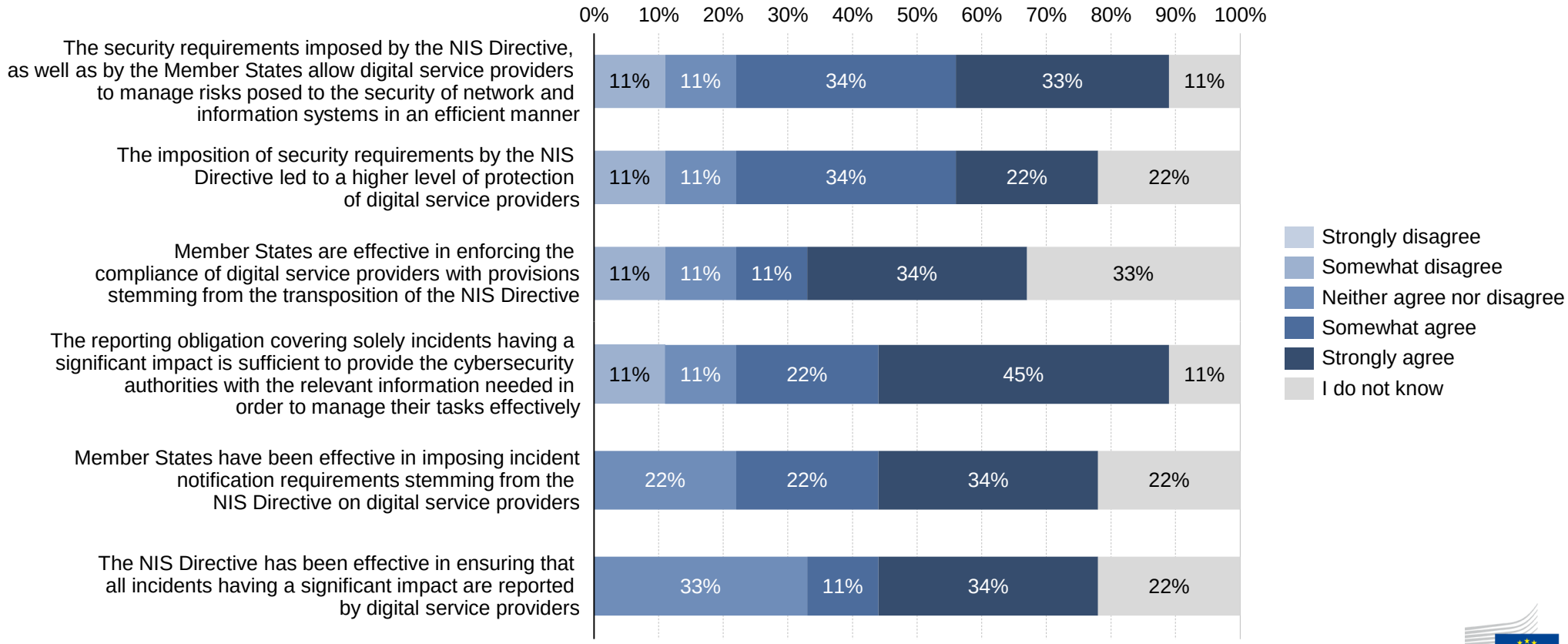
OESs respondents were asked **'To what extent would you agree with the following statements related to the security requirements and the incident notification provisions laid down in Article 14 of the Directive?'.** The histogram below shows the distribution of responses to the OESs online surveys:



Source: Targeted online survey conducted by Wavestone with OESs. N for OESs=49

Effectiveness – Security requirements and incident notification - DSPs

DSPs respondents were asked **'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?'.** The histogram below shows the distribution of responses to the DSPs online surveys:

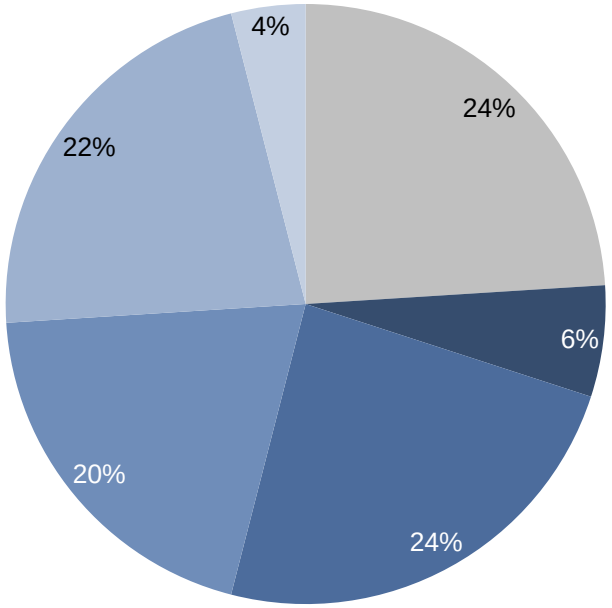


Source: Targeted online survey conducted by Wavestone with DSPs. N for DSPs=9

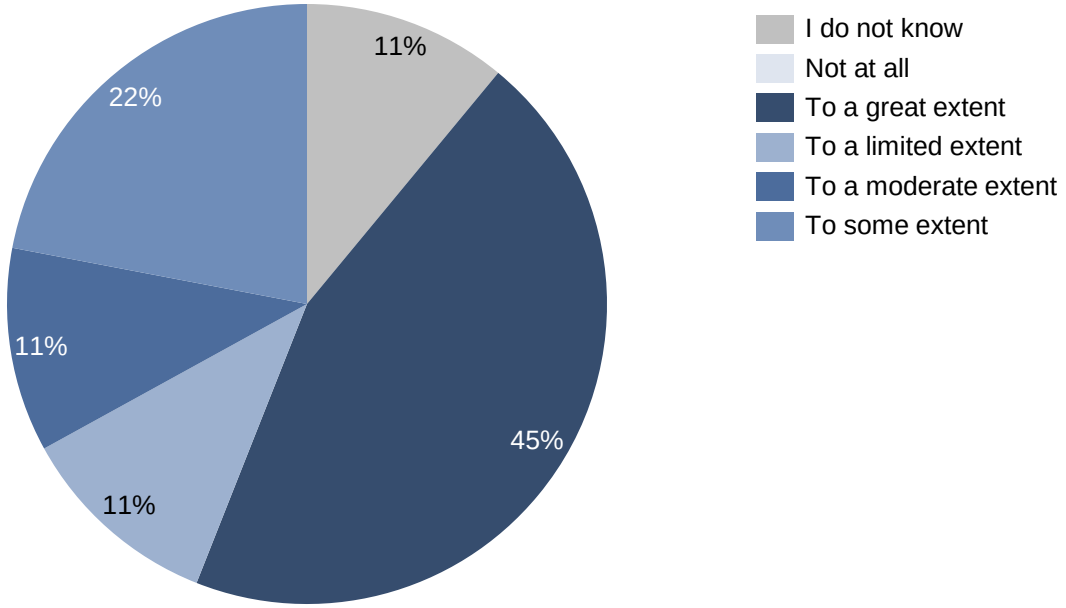
Effectiveness - Light touch approach towards DSPs

CAs and DSPs respondents were asked **'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?'.** The histogram below shows the distribution of responses to the Cas and DSPs online survey:

CAs



DSPs



Source: Targeted online survey conducted by Wavestone with CAs and DSPs. N for CAs=46; N for DSP=9

Efficiency - Costs

The criterion of efficiency evaluates whether the costs implied by the implementation of the NIS Directive are reasonable and proportionate to the benefits achieved.

Costs

From the findings of the **online surveys**, it emerged that **the administrative and compliance costs brought about by the NIS Directive was reasonable**.

During the **in-depth interviews**, the negative impact that the interviewees flagged as the most relevant when it comes to the implementation of the NIS Directive is the **duplication of efforts**, both in terms of human resources and time, **to comply with different legislation**, which often implies having different reporting authorities, timelines, and thresholds.

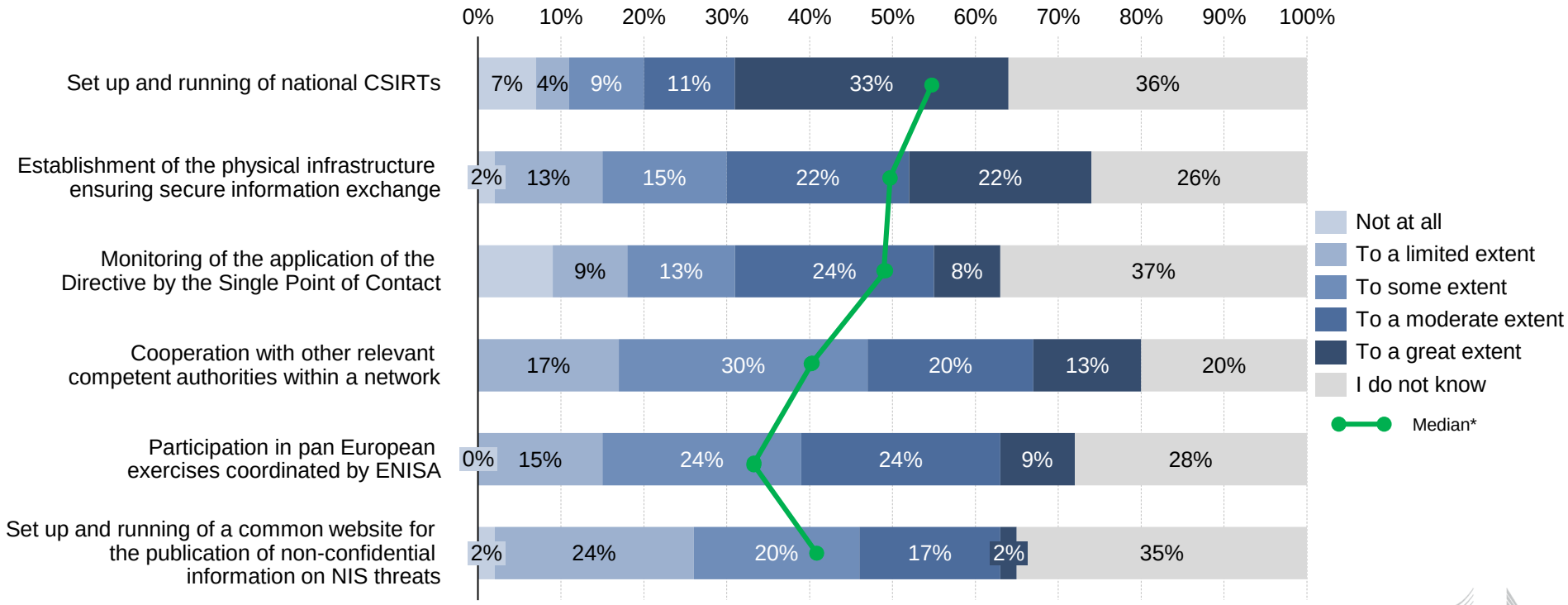
Benefits

Regarding the benefits, the NIS Directive ensured 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 benefit of the NIS Directive are the **increased trust in the digital economy, the improved functioning of the internal market, and the reduced impact of NIS incidents**.

Efficiency – Compliance Costs - CAs

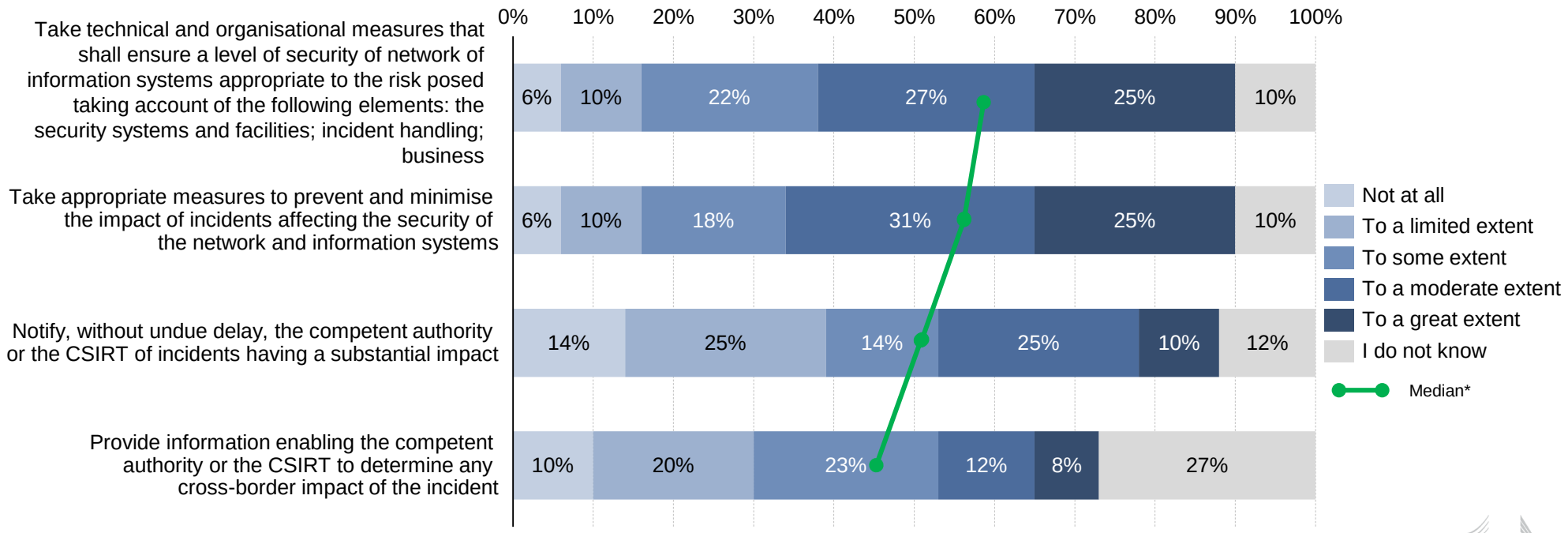
CAs respondents were asked '**Considering the following compliance costs with the provisions of the NIS Directive, to what extent are they significant for the competent authorities in your country?'.** Among **CAs**, the set up and running of national CSIRTs emerged as the most significant cost, followed by the establishment of the physical infrastructure ensuring secure information exchange. The histogram below shows the distribution of responses to the CAs online survey.



Source: Targeted online survey conducted by Wavestone with CAs. N for CAs=46.
*The median is a measure of where the center of a data set lies. The median was used as opposed to the mean to avoid that outliers in the sequence skewed the average of the values.

Efficiency – Compliance Costs - OESs

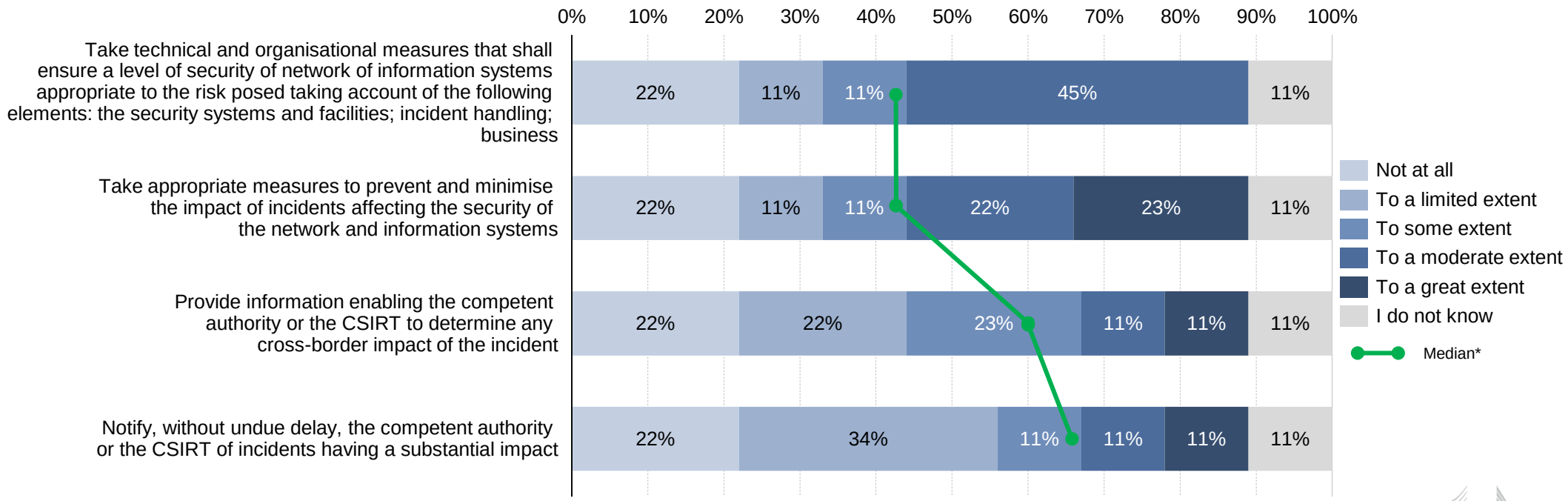
OESs respondents were asked '**Considering the following compliance costs with the provisions of the NIS Directive, to what extent are they significant for the competent authorities in your country?'. OESs** reported that taking appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems emerged as their major cost. The histogram below shows the distribution of responses to the OESs online survey.



Source: Targeted online survey conducted by Wavestone with OESs. N for OESs=49.
*The median is a measure of where the center of a data set lies. The median was used as opposed to the mean to avoid that outliers in the sequence skewed the average of the values.

Efficiency – Compliance Costs - DSPs

DSPs respondents were asked '**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?'. DSPs** reported that taking appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems emerged as their major cost. The histogram below shows the distribution of responses to the DSPs online survey.



Source: Targeted online survey conducted by Wavestone with DSPs. N for DSPs=9.
*The median is a measure of where the center of a data set lies. The median was used as opposed to the mean to avoid that outliers in the sequence skewed the average of the values.

Thank you