

Consultation on the revision of the NIS Directive

Fields marked with * are mandatory.

Introduction

As our daily lives and economies become increasingly dependent on digital technologies and internet-based services and products, we become more vulnerable and exposed to cyber-attacks. We are witnessing that the threat landscape is constantly evolving and the attack surface constantly expanding, putting network and information systems at greater risk than ever before. The COVID-19 crisis and the resulting growth in demand for internet-based solutions has emphasised even more the need for a state of the art response and preparedness for a potential future crisis. Maintaining a high level of cybersecurity across the European Union has become essential to keep the economy running and to ensure prosperity.

[Directive \(EU\) 2016/1148](#) concerning measures for a high common level of security of network and information systems across the Union (“NIS Directive” or “the Directive”) is the first horizontal internal market instrument aimed at improving the resilience of the EU against cybersecurity risks. Based on Article 114 of the Treaty on the Functioning of the European Union, the NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- a high level of preparedness of Member States by requiring them to designate one or more national Computer Security Incident Response Teams (CSIRTs) responsible for risk and incident handling and a competent national NIS authority;
- cooperation among all the Member States by establishing the Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States, and the CSIRTs network, which promotes swift and effective operational cooperation between national CSIRTs;
- a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure. Public and private entities identified by the Member States as operators of essential services in these sectors are required to undertake a risk assessment and put in place appropriate and proportionate security measures as well as to notify serious incidents to the relevant authorities. Also providers of key digital services such as search engines, cloud computing services and online marketplaces have to comply with the security and notification requirements under the Directive.

Article 23 of the NIS Directive requires the European Commission to review the functioning of this Directive periodically. As part of its key policy objective to make “Europe fit for the digital age” as well as in line with the objectives of the Security Union, the Commission announced in its Work Programme 2020 that it would

conduct the review by the end of 2020. This would advance the deadline foreseen under Article 23(2) of the Directive, according to which the Commission shall review the Directive for the first time and report to the European Parliament and the Council by 9 May 2021.

As part of this process, this consultation seeks your views on the topic of cybersecurity as well as on the different elements of the NIS Directive, which are all subject to the review. The results of this consultation will be used for the evaluation and impact assessment of the NIS Directive.

This consultation is open to everybody: citizens, public and private organisations, trade associations and academics. The questionnaire is divided in three sections:

- **Section 1** contains general questions on the NIS Directive that are accessible to all categories of stakeholders.
- **Section 2** contains technical questions on the functioning of the NIS Directive. This section is mainly targeted at individuals, organisations or authorities that are familiar with the NIS Directive and cybersecurity policies.
- **Section 3** aims to gather views on approaches to cybersecurity in the European context currently not addressed by the NIS Directive. This section is mainly targeted at individuals, organisations or authorities that are familiar with the NIS Directive and cybersecurity policies.

Written feedback provided in other document formats can be uploaded through the button made available at the end of the questionnaire.

The survey will remain open until 02 October 2020 - 23h00.

About you

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- Gaelic
- German
- Greek

- Hungarian
- Italian
- Latvian
- Lithuanian
- Maltese
- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as

- Academic/research institution
- Business association
- Company/business organisation
- Consumer organisation
- EU citizen
- Environmental organisation
- Non-EU citizen
- Non-governmental organisation (NGO)
- Public authority
- Trade union
- Other

* First name

Andreas

* Surname

KASTL

* Email (this won't be published)

andreas.kastl@vab.de

* Organisation name

255 character(s) maximum

Association of Foreign Banks in Germany

* Organisation size

- Micro (1 to 9 employees)
- Small (10 to 49 employees)
- Medium (50 to 249 employees)
- Large (250 or more)

Transparency register number

255 character(s) maximum

Check if your organisation is on the [transparency register](#). It's a voluntary database for organisations seeking to influence EU decision-making.

95840804-38

* Country of origin

Please add your country of origin, or that of your organisation.

- | | | | |
|---|--|-------------------------------------|--|
| <input type="radio"/> Afghanistan | <input type="radio"/> Djibouti | <input type="radio"/> Libya | <input type="radio"/> Saint Martin |
| <input type="radio"/> Åland Islands | <input type="radio"/> Dominica | <input type="radio"/> Liechtenstein | <input type="radio"/> Saint Pierre and Miquelon |
| <input type="radio"/> Albania | <input type="radio"/> Dominican Republic | <input type="radio"/> Lithuania | <input type="radio"/> Saint Vincent and the Grenadines |
| <input type="radio"/> Algeria | <input type="radio"/> Ecuador | <input type="radio"/> Luxembourg | <input type="radio"/> Samoa |
| <input type="radio"/> American Samoa | <input type="radio"/> Egypt | <input type="radio"/> Macau | <input type="radio"/> San Marino |
| <input type="radio"/> Andorra | <input type="radio"/> El Salvador | <input type="radio"/> Madagascar | <input type="radio"/> São Tomé and Príncipe |
| <input type="radio"/> Angola | <input type="radio"/> Equatorial Guinea | <input type="radio"/> Malawi | <input type="radio"/> Saudi Arabia |
| <input type="radio"/> Anguilla | <input type="radio"/> Eritrea | <input type="radio"/> Malaysia | <input type="radio"/> Senegal |
| <input type="radio"/> Antarctica | <input type="radio"/> Estonia | <input type="radio"/> Maldives | <input type="radio"/> Serbia |
| <input type="radio"/> Antigua and Barbuda | <input type="radio"/> Eswatini | <input type="radio"/> Mali | <input type="radio"/> Seychelles |
| <input type="radio"/> Argentina | <input type="radio"/> Ethiopia | <input type="radio"/> Malta | <input type="radio"/> Sierra Leone |

- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Morocco
- Mozambique
- Myanmar /Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia

- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Christmas Island
- Clipperton
- Cocos (Keeling) Islands
- Colombia
- Comoros
- Congo
- Cook Islands
- Costa Rica
- Côte d'Ivoire
- Croatia
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Italy
- Jamaica
- Japan
- Jersey
- Jordan
- Kazakhstan
- Kenya
- Kiribati
- Kosovo
- Kuwait
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Papua New Guinea
- Paraguay
- Peru
- Philippines
- Pitcairn Islands
- Poland
- Portugal
- Puerto Rico
- Qatar
- Réunion
- Romania
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Turkey
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine
- United Arab Emirates
- United Kingdom
- United States
- United States Minor Outlying Islands
- Uruguay
- US Virgin Islands
- Uzbekistan
- Vanuatu
- Vatican City
- Venezuela
- Vietnam

- Cuba
- Curaçao
- Cyprus
- Czechia
- Democratic Republic of the Congo
- Denmark
- Kyrgyzstan
- Laos
- Latvia
- Lebanon
- Lesotho
- Liberia
- Russia
- Rwanda
- Saint Barthélemy
- Saint Helena Ascension and Tristan da Cunha
- Saint Kitts and Nevis
- Saint Lucia
- Wallis and Futuna
- Western Sahara
- Yemen
- Zambia
- Zimbabwe

* Publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

Anonymous

Only your type of respondent, country of origin and contribution will be published. All other personal details (name, organisation name and size, transparency register number) will not be published.

Public

Your personal details (name, organisation name and size, transparency register number, country of origin) will be published with your contribution.

I agree with the [personal data protection provisions](#)

* Can you specify further your capacity in which you are replying to the questionnaire on the review of the NIS Directive?

- Citizen
- Centralised national competent authority in charge of supervision
- Sectoral national competent authority in charge of supervision
- National CSIRT
- Other national competent authority
- EU body
- Operator of essential services currently covered by the NIS Directive

- Digital service provider currently covered by the NIS Directive
- Economic operator currently not covered by the NIS Directive
- Trade association representing entities currently covered by the NIS Directive
- Trade association representing entities currently not covered by the NIS Directive
- Trade association representing both entities currently covered and entities not covered by the NIS Directive
- Academia
- Cybersecurity professional
- Consumer organisation
- Other

Please specify the sector you are responsible for:

Banking, Financial Services

* Before starting this survey, are you aware of the [objectives and principles](#) of the EU Directive on security of network and information systems (the NIS Directive)?

- Not aware at all
- Slightly aware
- Aware
- Strongly aware
- Don't know / no opinion

* Has your organisation been impacted by the adoption of the NIS Directive (for example by having to adopt certain measures stemming directly from the Directive or from national laws transposing the Directive, or by participating in the various cooperation fora established by the Directive)?

- Yes
- No
- Don't know / no opinion

Section 1: General questions on the NIS Directive

Sub-section 1.a. – Relevance of the NIS Directive

The NIS Directive envisages to (1) increase the capabilities of Member States when it comes to mitigating cybersecurity risks and handling incidents, (2) improve the level of cooperation amongst Member States in

the field of cybersecurity and the protection of essential services, and (3) promote a culture of cybersecurity across all sectors vital for our economy and society.

Q1: To what extent are these objectives still relevant?

	Not relevant at all	Not relevant	Relevant	Very relevant	Don't know / no opinion
Increase the capabilities of Member States	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Improve the level of cooperation amongst Member States	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Promote a culture of security across all sectors vital for our economy and society	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sub-section 1.b. – Cyber-threat landscape

Q1: Since the entry into force of the NIS Directive in 2016, how has in your opinion the cyber threat landscape evolved?

- Cyber threat level has decreased significantly
- Cyber threat level has decreased
- Cyber threat level is the same
- Cyber threat level has increased
- Cyber threat level has increased significantly
- Don't know / no opinion

Q2: How do you evaluate the level of preparedness of small and medium-sized companies in the EU against current cyber threats (on a scale from 1 to 5 with 5 indicating that companies score highly on cyber resilience)?

- 1
- 2
- 3
- 4
- 5
- Don't know / no opinion

Sub-section 1.c. – Technological advances and new trends

Technological advances and new trends provide great opportunities to the economy and society as a whole. The growing importance of edge computing (which is a new model of technology deployment that

brings data processing and storage closer to the location where it is needed, to improve response times and save bandwidth), as well as the high reliance on digital technologies especially during the COVID-19 crisis increases at the same time the potential attack surface for malicious actors. All this changes the paradigm of security resulting in new challenges for companies to adapt their approaches to ensuring the cybersecurity of their services.

Q1: In which way should such recent technological advances and trends be considered in the development of EU cybersecurity policy?

1000 character(s) maximum

The cyber-threat situation has steadily increased in recent years. However, the NIS Directive should remain open to technological solutions in order to ensure a stable legal situation in the long term.

Sub-section 1.d. – Added-value of EU cybersecurity rules

The NIS Directive is based on the idea that common cybersecurity rules at EU level are more effective than national policies alone and thus contribute to a higher level of cyber resilience at Union level.

Q1: To what extent do you agree with the following statements?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Cyber risks can propagate across borders at high speed, which is why cybersecurity rules should be aligned at Union level	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The mandatory sharing of cyber risk related information between national authorities across Member States would contribute to a higher level of joint situational awareness when it comes to cyber risks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
All entities of a certain size providing essential services to our society should be subject to similar EU-wide cybersecurity requirements	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Sub-section 1.e. – Sectoral scope

Under the current NIS Directive, certain public and private entities are required to take appropriate security measures and notify serious incidents to the relevant national authorities. Entities subject to these requirements include so-called operators of essential services (OES) and digital service providers (DSP).

Operators of essential services are entities operating in seven sectors and subsectors: energy (electricity, oil and gas), transport (air, rail, water and road), banking, financial market infrastructures, health sector, drinking water supply and distribution, and digital infrastructure (IXPs, DNS providers and TLD registries). Digital service providers are either cloud service providers, online search engines or online marketplaces.

Q1: Should the following sectors or services be included in the scope of the Directive due to their exposure to cyber threats and their importance for the economy and the society as a whole?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Public administration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Food supply	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Manufacturing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Chemicals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Waste water	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Social networks	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Data centres	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q2: Should undertakings providing public communications networks or publically available electronic communications services currently covered by the security and notification requirements of the EU telecom framework be included in the scope of the NIS Directive?

- Yes
- No
- Don't know / no opinion

Q3: Do you consider that also other sectors, subsectors and/or types of digital services need to be included in the scope of the Directive due to their exposure to cyber threats and their importance for the economy and the society as a whole?

- Yes
- No
- Don't know / no opinion

Sub-section 1.f. – Regulatory treatment of OES and DSPs by the NIS Directive

As regards the imposition of security and notification requirements, the NIS Directive distinguishes between two main categories of economic entities: operators of essential services (OES) and digital service providers (DSP). While in the case of OES, Member States are allowed to impose stricter security and notification requirements than those enshrined in the Directive, they are prohibited to do so for DSPs. Moreover, competent authorities can only supervise DSPs "ex-post" (when an authority is provided with evidence that a company does not fulfil its obligations) and not "ex-ante" as in the case of OES. These are

elements of the so-called "light-touch" regulatory approach applied towards DSPs, which was motivated by the lower degree of risk posed to the security of the digital services and the cross-border nature of their services.

Q1: Do you agree that the "light-touch" regulatory approach applied towards DSPs is justified and therefore should be maintained?

- Yes
- No
- Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

Sub-section 1.g. – Information sharing

Under the NIS Directive, Member States must require operators of essential services (OES) and digital service providers (DSP) to report serious incidents. According to the Directive, incidents are events having an actual adverse effect on the security of network and information systems. As a result, reportable incidents constitute only a fraction of the relevant cybersecurity information gathered by OES and DSPs in their daily operations.

Q1: Should entities under the scope of the NIS Directive be required to provide additional information to the authorities beyond incidents as currently defined by the NIS Directive?

- Yes
- No
- Don't know / no opinion

Section 2: Functioning of the NIS Directive

Sub-section 2.a. – National strategies

The NIS Directive requires Member States to adopt national strategies on the security of network and information systems defining strategic objectives and policy measures to achieve and maintain a high level of cybersecurity and covering at least the sectors referred to in Annex II and the services referred to in Annex III of the Directive.

Q1: In your opinion, how relevant are common objectives set on EU level for the adoption of national strategies on the security of network and information systems in order to achieve a high level of cybersecurity?

- Not relevant at all
- Not relevant
- Relevant
- Very relevant
- Don't know / no opinion

Q2: Taking into account the evolving cybersecurity landscape, should national strategies take into account any additional elements so far not listed in the Directive?

- Yes
- No
- Don't know / no opinion

Sub-section 2.b. – National competent authorities and bodies

The Directive requires Member States to designate one or more national competent authorities on the security of network and information systems to monitor the application of the Directive on a national level. In addition, Member States are required to appoint a single point of contact to ensure cross-border cooperation with the relevant authorities in other Member States and with the Cooperation Group and the CSIRT network as well as one or more computer security incident response teams (CSIRTs) responsible for risk and incident handling for the sectors and services covered by Annex II and III of the Directive.

Q1: In your opinion what is the impact of the NIS Directive on national authorities dealing with the security of network and information systems in the Member States?

	No impact	Low impact	Medium impact	High impact	Don't know / no opinion
Level of funding	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Level of staffing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Level of expertise	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperation of authorities across Member States	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cooperation between national competent authorities within Member States	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q2: In your opinion, what is the impact of the NIS Directive on national Computer Security Incident Response Teams (CSIRTs) in the Member States?

	No impact	Low impact	Medium impact	High impact	Don't know / no opinion
Level of funding	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Level of staffing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Level of operational capabilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Level of expertise	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cooperation with OES and DSP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cooperation with relevant national authorities (such as sectoral authorities)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q3: How do you evaluate the quality of services provided by the national Computer Security Incident Response Teams to OES (on a scale from 1 to 5 with 5 indicating a very high level of quality)?

- 1
- 2
- 3
- 4
- 5
- Don't know / no opinion

Q4: How do you evaluate the quality of services provided by the national Computer Security Incident Response Teams to DSPs (on a scale from 1 to 5 with 5 indicating a very high level of quality)?

- 1
- 2
- 3
- 4
- 5
- Don't know / no opinion

Q5: Under the NIS Directive, competent authorities or the CSIRTs shall inform the other affected Member State(s) if an incident has a significant impact on the continuity of essential services in that Member State. How do you evaluate the

level of incident-related information sharing between Member States (on a scale from 1 to 5 with 5 indicating a very high degree of satisfaction with the information shared)?

- 1
- 2
- 3
- 4
- 5
- Don't know / no opinion

Q6: If you are an OES/DSP: Has your organisation received technical support from the national CSIRTs in case of an incident?

- Yes
- No
- Don't know / no opinion

Q7: Should the CSIRTs be assigned additional tasks so far not listed in the NIS Directive?

- Yes
- No
- Don't know / no opinion

Q8: How do you evaluate the functioning of the single points of contact (SPOCs) since their establishment by the NIS Directive as regards the performance of the following tasks (on a scale from 1 to 5 with 5 indicating a very high level of performance)?

	1	2	3	4	5	Don't know / no opinion
Cross-border cooperation with the relevant authorities in other Member States	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cooperation with the Cooperation Group	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cooperation with the CSIRTs network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q9: Should the single points of contact be assigned additional tasks so far not listed in the NIS Directive?

- Yes
- No
- Don't know / no opinion

Q10: How do you evaluate the level of consultation and cooperation between competent authorities and SPOCs on the one hand, and relevant national law enforcement authorities and national data protection authorities on the other hand (on a scale from 1 to 5 with 5 indicating a very high level of cooperation)?

- 1
- 2
- 3
- 4
- 5
- Don't know / no opinion

Sub-section 2.c. – Identification of operators of essential services and sectoral scope

Operators of essential services are organisations that are important for the functioning of the economy and society as a whole. While the NIS Directive provides a list of sectors and subsectors, in which particular types of entities could become subject to security and incident reporting requirements, Member States are required to identify the concrete operators for which these obligations apply by using criteria set out in the Directive.

Q1: To what extent do you agree with the following statements regarding the concept of identification of operators of essential services (OES) introduced by the NIS Directive and its implementation by Member States?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
The current approach ensures that all relevant operators are identified across the Union.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
OES are aware of their obligations under the NIS Directive.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Competent authorities actively engage with OES.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

The cross-border consultation procedure in its current form is an effective element of the identification process to deal with cross-border dependencies.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The identification process has contributed to the creation of a level playing field for companies from the same sector across the Member States.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please elaborate your answer:

1000 character(s) maximum

In general, the current approach of the NIS Directive should theoretically ensure that all relevant operators are identified in a uniform or at least harmonised way across the Union. In the case of the banking sector, the Annex II of the Directive lists under number 3 that credit institutions as defined in Art. 4 para. 1 No. 1 of Regulation (EU) No 575/2013 (so-called CRR) are to be considered potential operators of essential services. In this regard, we advise an amendment to number 3 of Annex II of the Directive stating that the “small and non-complex institutions” in the meaning of Art. 4 para. 1 no. 145 CRR are not potential operators of essential services. According to Art. 5 of the Directive, the Member States shall identify the operators of essential services. This has led to a situation in which the proceedings to identify those operators varies a lot across Member States. [

Q2: Given the growing dependence on ICT systems and the internet in all sectors of the economy, to what extent do you agree with the following statements regarding the scope of the NIS Directive when it comes to operators of essential services?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Definitions of the types of entities listed in Annex II are sufficiently clear.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
More sectors and sub-sectors should be covered by the Directive.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Identification thresholds used by Member States should be lower (i.e. more companies should be covered).	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please elaborate your answers:

1000 character(s) maximum

Q3: If you agree with the statement above that more sectors and sub-sectors should be covered by the Directive, which other sectors should be covered by the scope of the NIS Directive and why?

1000 character(s) maximum

Q4: How has the level of risk of cyber incidents in the different sectors and subsectors covered by the NIS Directive evolved since the Directive entered into force in 2016?

	Very significant decrease in risk	Significant decrease in risk	No increase or decrease in risk	Significant increase in risk	Very significant increase in risk	Don't know / no opinion
Electricity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Oil	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Gas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Air transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rail transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Water transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Road transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Banking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Financial market infrastructures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health sector	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Drinking water supply and distribution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital infrastructure (IXPs, DNS providers, TLD registries)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q5: How do you evaluate the level of cybersecurity resilience when it comes to the different sectors and subsectors covered by the NIS Directive?

	Very low	Low	Medium	High	Very high	Don't know / no opinion
Electricity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Oil	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Gas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Air transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Rail transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Water transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Road transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Banking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Financial market infrastructures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health sector	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Drinking water supply and distribution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Digital infrastructure (IXPs, DNS providers, TLD registries)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Q6: How do you evaluate the level of cyber resilience and the risk-management practices applied by those small and medium-sized companies that are not covered by the NIS Directive (on a scale from 1 to 5 with 5 indicating that companies score highly on cyber resilience)?

	1	2	3	4	5	Don't know / no opinion
Small companies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Medium-sized companies	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Please elaborate your answers for both small and medium-sized companies:

	Your elaboration:
Small companies	
Medium-sized companies	

Q7: Do you think that the level of resilience and the risk-management practices applied by companies differ from sector to sector for small and medium-sized companies?

- Yes
- No
- Don't know / no opinion

If yes, please elaborate:

1000 character(s) maximum

On 28 November 2019, the European Banking Authority (EBA) published Guidelines on ICT and security risk management which established harmonised requirements for credit institutions, investment firms and payment service providers (PSPs) on the mitigation and management of their information and communication technology (ICT) and security risks. Although the Guidelines are to be applied in a proportionate way, all in all they will lead to a consistent and high level of ICT security in all financial market companies affected. Therefore, also small financial market companies will show a higher level of preparation and awareness as small enterprises from other non or less regulated economic sectors.

Sub-section 2.d. – Digital service providers and scope

Digital service providers (cloud service providers, online search engines and online marketplaces) shall also put in place security measures and report substantial incidents. For this type of entities, the Directive envisages a "light-touch" regulatory approach, which means inter alia that competent authorities can only supervise DSPs "ex-post" (when an authority is provided with evidence that a company does not fulfil its obligations). Member States are not allowed to impose any further security or reporting requirements than those set out in the Directive ("maximum harmonisation"). Jurisdiction is based on the criterion of main establishment in the EU.

Q1: To what extent do you agree with the following statements regarding the way in which the NIS Directive regulates digital service providers (DSPs)?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Annex III of the NIS Directive covers all relevant types of digital services.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Definitions of the types of digital services listed in Annex III are sufficiently clear.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
DSPs are aware of their obligations under the NIS Directive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Competent authorities have a good overview of the DSPs falling under their jurisdiction.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Competent authorities actively engage with DSPs under their jurisdiction.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Security requirements for DSPs are sufficiently harmonised at EU level.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Incident notification requirements for DSPs are sufficiently harmonised at EU level.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Reporting thresholds provided by the Implementing Regulation laying down requirements for Digital Service Providers under the NIS Directive are appropriate.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q2: If you disagree with the statement above that Annex III of the NIS Directive covers all relevant types of digital services, which other types of providers of digital services should fall under the scope of the NIS Directive and why ?

1000 character(s) maximum

Q3: To what extent do you agree with the following statements regarding the so-called “light-touch approach” of the NIS Directive towards digital service providers (DSPs)?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
The more harmonised regulatory approach applied towards DSPs as compared to OES is justified by the cross-border nature of their services.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Subjecting DSPs to the jurisdiction of the Member State where they have their main establishment in the EU minimises the compliance burden for those companies.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
The limitation related to the supervisory power of the national authorities, notably to take action only when provided with evidence (ex-post supervision), in the case of the DSPs is justified by the nature of their services and the degree of cyber risk they face.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
The exclusion of micro- and small enterprises is reasonable considering the limited impact of their services on the economy and society as a whole.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Please elaborate your answers:

1000 character(s) maximum

Q4: How do you evaluate the level of preparedness of digital service providers covered by the NIS Directive when it comes to cybersecurity related risks?

	Very low	Low	Medium	High	Very high	Don't know / no opinion
Online marketplaces	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Online search engines	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Cloud computing services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q5: In the previous question, you have been asked about the level of preparedness of different types of digital service providers. Please explain your assessment of the level of preparedness:

	Your explanation:
Online marketplaces	
Online search engines	
Cloud computing services	

Q6: How has the level of risk of cyber incidents in the different sectors and subsectors covered by the NIS Directive evolved since the Directive entered into force in 2016?

	Very significant decrease in risk	Significant decrease in risk	No increase or decrease in risk	Significant increase in risk	Very significant increase in risk	Don't know / no opinion
Online marketplaces	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Online search engines	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cloud computing services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q7: How do you evaluate the level of cybersecurity resilience when it comes to the different types of digital service providers covered by the NIS Directive?

	Very low	Low	Medium	High	Very high	Don't know / no opinion
Online marketplaces	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Online search engines	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cloud computing services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Sub-section 2.e. – Security requirements

Member States are required to ensure that entities take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems.

Q1: What is the impact of imposing security requirements on OES by the NIS Directive in terms of cyber resilience?

- No impact
- Low impact
- Medium impact
- High impact
- Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

The implementation of the contents of the NIS Directive has surely lead to more awareness and to more enhanced efforts of operators of essential services to establish IT security across all sectors. Besides this, it must also be stated that certain regulatory requirements for the banking and ficial industry have had a comparable effect on their own, on the one side in a very general manner as for example with regards to effective control systems and sound internal governance, and on the other side very disticntice and special as the already mentioned EBA Guidelines on ICT and security risk management of 28 November 2019.

Q2: What is the impact of imposing security requirements on DSPs by the NIS Directive in terms of cyber resilience?

- No impact
- Low impact
- Medium impact
- High impact
- Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

Q3: To what extent do you agree with the following statements regarding the implementation of security requirements under the NIS Directive?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Member States have established effective security requirements for OES on a national level.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
There is a sufficient degree of alignment of security requirements for OES and DSPs in all MS.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Please elaborate your answers:

1000 character(s) maximum

With regards to Member State where our association is domiciled, we could agree to both questions. But it is very difficult to find ground for statements on the implementation of security requirements under the NIS Directive in all other 26 Member States.

Are there sectoral differences for OES regarding how effectively security requirements have been put in place by the Member States?

- Yes
- No
- Don't know / no opinion

If yes, please specify for which sectors and elaborate:

1000 character(s) maximum

At least in the case of Germany, for every sector one (or even more) sector-specific requirements (so-called "B3S") have been developed respectively are still under development.

Q4: While some Member States have put in place rather general security requirements, other Member States have enacted very detailed requirements featuring a higher degree of prescriptiveness. To what extent do you agree with the following statements regarding these different approaches?

					Don't know /

	Strongly disagree	Disagree	Agree	Strongly agree	no opinion
Prescriptive requirements make it easy for companies to be compliant.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prescriptive requirements leave too little flexibility to companies.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prescriptive requirements ensure a higher level of cybersecurity than general risk management obligations.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Prescriptive requirements make it difficult to take into account technological progress, new approaches to doing cybersecurity and other developments.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The different level of prescriptiveness of requirements increases a regulatory burden for companies operating across different national markets.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The companies should have the possibility to use certification to demonstrate compliance with the NIS security requirements.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The companies should be required to use certification for their compliance with NIS security requirements.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please elaborate your answers:

1000 character(s) maximum

In the case of a company that has been identified as an operator of essential services in more than one Member State and in the case of a groups of companies whose (sub)entities have been identified as an operator of essential services in more than one Member State, varying regulatory requirements and in the end also different level of prescriptiveness of such requirements increase regulatory burdens for companies operating across different national markets. In this regard, it might be useful to transpose certain contents of the Directive into a newly EU Regulation concerning measures for a high common level of security of network and information systems across the Union.

Sub-section 2.f. – Incident notification

Member States are required to ensure that entities notify the competent authority or the CSIRT of incidents having a significant impact on the continuity or provision of services.

Q1: To what extent do you agree with the following statements regarding the implementation of notification requirements under the NIS Directive?

--	--	--	--

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
The majority of companies have developed a good understanding of what constitutes an incident that has to be reported under the NIS Directive.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Member States have imposed notification requirements obliging companies to report all significant incidents.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The current approach ensures that OES across the Union face sufficiently similar incident notification requirements.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Please elaborate your answers:

1000 character(s) maximum

In the case of a company that has been identified as an operator of essential services in more than one Member State and in the case of a groups of companies whose (sub)entities have been identified as an operator of essential services in more than one Member State, varying regulatory requirements of the Member States lead also to different definitions and conditions that must be observed and complied with in order to establish and maintain appropriate incident reporting facilities and capabilities. Therefore, we highly appreciate that the September 2020 Commission proposal for a regulation on digital and operational resilience at least entails in Article 19 a provision for a centralised reporting of major ICT-related incidents.

Sub-section 2.g. – Level of discretion on transposition and implementation given to Member States

The NIS Directive gives a wide room of discretion to Member States when it comes to the identification of operators of essential services, the setting of security requirements and the rules governing incident notification.

Q1: To what extent do you agree with the following statements regarding this approach from an internal market perspective?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion

The approach leads to significant differences in the application of the Directive and has a strong negative impact on the level playing field for companies in the internal market.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The approach increases costs for OES operating in more than one Member State.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
The approach allows Member States to take into account national specificities.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Please elaborate your answers:

1000 character(s) maximum

We absolutely agree to the first two questions, also as it represents an older result of the Commission’s 2019 report assessing the consistency of the approaches in the identification of operators of essential services was that it recommended Member States to consult each other in order to ensure that cross-border operators face similar security and incident reporting requirements in the internal market. More legal certainty for operators that are active in more than one Member State may be reached by a new EU Regulation concerning measures for a high common level of security of network and information systems across the Union.

Sub-section 2.h. – Enforcement

The Directive requires Member States to assess the compliance of operators of essential services with the provisions of the Directive. They must also ensure that competent authorities act when operators of essential services or digital service providers do not meet the requirements laid down in the Directive. Member States must also lay down rules for penalties that are effective, proportionate and dissuasive.

Q1: To what extent do you agree with the following statements regarding national enforcement of the provisions of the NIS Directive and its respective national implementations?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Member States are effectively enforcing the compliance of OES.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Member States are effectively enforcing the compliance of DSPs.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
The types and levels of penalties set by Member States are effective, proportionate and dissuasive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
There is a sufficient degree of alignment of penalty levels between the different Member States.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Sub-section 2.i. – Information exchange

The NIS Directive has created two new fora for information exchange: the Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States, and the CSIRTs network, which promotes swift and effective operational cooperation between national CSIRTs.

Q1: To what extent do you agree with the following statements regarding the functioning of the Cooperation Group and the CSIRTs network?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
The Cooperation Group has been of significant help for the Member States to implement the NIS Directive.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The Cooperation Group has played an important role in aligning national transposition measures.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
The Cooperation Group has been instrumental in dealing with general cybersecurity matters.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The Cooperation Group is dealing with cross-border dependencies in an effective manner.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
The CSIRTs network has effectively managed to fulfil its tasks as laid down in the NIS Directive.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
The CSIRTs network has helped to build confidence and trust amongst its members.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
The CSIRTs network has achieved swift and effective operational cooperation.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
The Cooperation Group and the CSIRTs network cooperate effectively.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q2: Should the Cooperation Group be assigned additional tasks so far not listed in the NIS Directive?

- Yes
- No
- Don't know / no opinion

If yes, please specify which tasks:

500 character(s) maximum

Although the 2019 Guidelines for the Member States on voluntary information exchange on cross-border dependencies may be seen as a first step for more harmonised information exchange, we did not have the impression that efforts of the NIS Cooperation Group alone can lead to an improvement on current cross-border deficiencies in this regard, and we therefore advocate for more uniform requirements on EU level, or otherwise for more direct powers for Level 2 measures to be adopted by the Group.

Q3: Should the CSIRTs network be assigned additional tasks so far not listed in the NIS Directive?

- Yes
- No
- Don't know / no opinion

Sub-section 2.j. – Efficiency of the NIS Directive

Q1: To what extent have the effects of the NIS Directive been achieved at a reasonable cost? To what extent are the costs of the intervention justified and proportionate given the benefits it has achieved?

- Not at all
- To a little extent
- To some extent
- To a large extent
- Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

Q2: What impact has the NIS Directive had on the overall level of resilience against cyber-threats across the EU when it comes to entities providing services that are essential for the maintenance of critical societal and economic activities?

- No impact
- Low impact
- Medium impact
- High impact
- Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

Sub-section 2.k. – Coherence of the NIS Directive with other EU legal instruments

The NIS Directive is not the only legal instrument on EU level that seeks to ensure more security of our digital environment. EU laws such as the General Data Protection Regulation or the European Electronic Communications Code are pursuing similar objectives.

Q1: To what extent are the provisions of the NIS Directive (such as on security requirements and incident notification) coherent with the provisions of other EU legal instruments that are aimed at increasing the level of data protection or the level of resilience?

- 1
- 2
- 3
- 4
- 5
- Don't know / no opinion

Please elaborate your answer:

1000 character(s) maximum

Section 3: Approaches to cybersecurity in the European context currently not addressed by the NIS Directive

Sub-section 3.a. – Provision of cybersecurity information

Pursuant to the provisions of NIS Directive, Member States have to require operators of essential services and digital service providers to report incidents above certain thresholds. However, organisations collect a lot of valuable information about cybersecurity risks that do not materialise into reportable incidents.

Q1: How could organisations be incentivised to share more information with cybersecurity authorities on a voluntary basis?

1000 character(s) maximum

- (-) Lean and simple reporting channels (established structures and procedures should be used for this purpose, coordinating function: competent national authorities) ,
 - (-) standardised reporting forms,
 - (-) confidential exchange of information between both operators and competent authorities

- (-) do not give the operators the feeling of operating an informative "one-way street" where the authorities receive a lot of information but the operators are not or hardly ever provided with the resulting findings.
- (-) Perhaps ensure anonymity of the person reporting

Q2: Under the NIS Directive, Member States shall require companies to report events having an actual adverse effect on the security of network and information systems (incidents). Should the reporting obligations be broadened to include other types of information in order to improve the situational awareness of competent authorities?

- Yes
- No
- Don't know / no opinion

Q3: The previous two questions have explored ways of improving the information available to cybersecurity authorities on national level. Which information gathered by such authorities should be made available on European level to improve common situational awareness (such as incidents with cross-border relevance, statistical data that could be aggregated by a European body etc.)?

1000 character(s) maximum

We support the pooling of national knowledge and further analysis of cyber threat scenarios from a European and strategic perspective. The lessons learned should result in regular (semi-annual) reports on the current cyber security situation. This should take into account all relevant information, such as technical information, incidents, attack strategies, statistical information and other sources and types of information in an anonymous and aggregated form.

Sub-section 3.b. –Information exchange between companies

Some Member States have fostered the development of fora where companies can exchange information about cybersecurity. This includes inter alia public private partnerships (PPP) or sectorial Information Sharing and Analysis Centres (ISACs). To some extent, such fora also exist on European and international level.

Q1: How would you evaluate the level of information exchange between organisations in their respective sectors when it comes to cybersecurity?

	Very low level	Low level	Medium level	High level	Very high level	Don't know / no opinion
Electricity	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Oil	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Gas	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Air transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Rail transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Water transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Road transport	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Banking	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Financial market infrastructures	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Health sector	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Drinking water supply and distribution	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Digital infrastructure (IXPs, DNS providers, TLD registries)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Digital service providers (online marketplaces)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Digital service providers (online search engines)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Digital service providers (cloud computing services)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Q2: How would you evaluate the level of information exchange between organisations across sectors when it comes to cybersecurity?

- Very low level
- Low level
- Medium level
- High level
- Very high level
- Don't know / no opinion

Q3: How could the level of information exchange between companies be improved within Member States but also across the European Union?

1000 character(s) maximum

Sub-section 3.c. – Vulnerability discovery and coordinated vulnerability disclosure

While the negative impact of vulnerabilities present in ICT products and services is constantly increasing, finding and remedying such vulnerabilities plays an important role in reducing the overall cybersecurity risk. Cooperation between organisations, manufacturers or providers of ICT products and services, and members of the cybersecurity research community and governments who find vulnerabilities has been

proven to significantly increase both the rate of discovery and the remedy of vulnerabilities. Coordinated vulnerability disclosure specifies a structured process of cooperation in which vulnerabilities are reported to the owner of the information system, allowing the organisation the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties or to the public. The process also provides for coordination between the finder and the organisation as regards the publication of those vulnerabilities.

Some Member States have put in place coordinated vulnerability disclosure policies that further facilitate the cooperation of all involved stakeholders.

Q1: How do you evaluate the level of effectiveness of such national policies in making vulnerability information available in a more timely manner?

- Very low level
- Low level
- Medium level
- High level
- Very high level
- Don't know / no opinion

Q2: Have you implemented a coordinated vulnerability disclosure policy?

- Yes
- No
- Don't know / no opinion
- Not applicable

Q3: How would you describe your experience with vulnerability disclosure in the EU and how would you improve it?

1000 character(s) maximum

Q4: Should national authorities such as CSIRTs take proactive measures to discover vulnerabilities in ICT products and services provided by private companies?

1000 character(s) maximum

Sub-section 3.d. – Security of connected products

The constantly growing proliferation of connected products creates enormous opportunities for businesses and citizens but it is not without its challenges: a security incident affecting one ICT product can affect the whole system leading to severe impacts in terms of disruption to economic and social activities.

Q1: Do you believe that there is a need of having common EU cybersecurity rules for connected products placed on the internal market?

- Yes
- No
- Don't know / no opinion

Sub-section 3.e. – Measures to support small and medium-sized enterprises and raise awareness

A few Member States have taken measures to raise the levels of awareness and understanding of cyber risk amongst small and medium-sized enterprises. Some Member States are also supporting such companies in dealing with cyber risk (for example by disseminating warnings and alerts or by offering training and financial support).

Q1: To what extent do you agree with the following statements regarding such measures?

	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
Such measures have proven to be effective in increasing the level of awareness and protection amongst SMEs.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
European legislation should require Member States to put in place frameworks to raise awareness amongst SMEs and support them.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Closing section: Submit your responses (and possibility to upload a document)

Thank you for your contribution to this questionnaire. In case you want to share further ideas on these topics, you can upload a document below.

Please upload your file

The maximum file size is 1 MB

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

d9165b25-d8ce-40b4-a9aa-3e96ff2dc701/VAB_NIS_Directive_Review_02102020.pdf

Contact

CNECT-H2@ec.europa.eu