Position Paper

Response to European Commission consultation on the review of the NIS Directive

Our reference:	EXCO-CS-20-052	Date:	5 October 2020
Referring to:	Cybersecurity – review of EU rules on the security of network and information systems		
Contact person:	Áine Clarke, Policy Advisor, General Insurance	E-mail:	Clarke@insuranceeurope.eu
Pages:	23	Transparency Register ID no.:	33213703459-54

Introductory remarks

- Insurance Europe welcomes the European Commission's ambitions to increase the Network and Information Security of sectors that are critical to the EU society and economy, as these sectors are vital for the everyday activities of businesses and consumers.
- The insurance industry, like other sectors, is embracing the digital transformation – both in terms of the opportunities and challenges it presents – and understands the vital importance of ensuring that the sector is resilient to attacks on its ICT systems (as evidenced in Insurance Europe's response to the European Commission consultation on a financial sector-specific digital operational resilience framework).
- The insurance business model is characterised by both shorter and longer-term operations. Insurers offer 'short-term' day-to-day services to their clients, the provision of which would indeed be disrupted by an incident involving an insurer's ICT systems. In this regard, the experience of insurance companies during the COVID-19 pandemic provides valuable insight into the measures taken by insurers to protect the more critical 'short term' services they provide, which will be outlined in more detail below. On the other hand, the criticality of the 'longer term' services provided by insurers cannot be compared with that of the sectors currently under the scope of the Directive (such as the energy, water, telecommunications or banking sectors), as a cyber incident within an insurance company would not have significant disruptive effects on the longer-term risk-transfer services it provides, in the way that an incident within any one of the aforementioned sectors would have a severe and immediate impact on business and consumer activity.
- The COVID-19 pandemic has presented itself as the ultimate stress test of ICT infrastructure and the preparedness of insurance companies. In general, insurers responded to national lockdown orders and/or recommendations to maintain social distancing by moving their combined workforce of over 900,000 employees to teleworking and setting up effective protocols to facilitate this transition. They implemented contingency plans to protect their customers and employees while minimising service interruptions. This process has been deployed with the maximum level of efficiency possible, although networks and ICT systems have been stretched, like in other sectors. Since insurers transitioned to the new COVID-19 working environment, one major cyber incident involving the industry has been reported, involving a large Spanish insurance company that fell victim to a cyberattack in August

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

2020. No data were lost as a result of the attack and the company in question recovered 90 percent of its services within a very short timeframe, recovering 100 percent of its services soon afterwards. The speed and efficiency of this response demonstrates that the possibility of such an attack was already provided and prepared for in the company's business impact analysis. Thanks to this, the event resulted in minimal disruption of services for clients. There have been no other incidents reported – of any size or involving any profile of insurer – and, on the contrary, a survey conducted by one national insurance association has drawn the conclusion that the industry was well-positioned to respond to the ICT challenges brought on by the pandemic. In other words, the ICT security and contingency programmes *put* in place by European (re)insurers have proven to be robust when confronted with the new COVID-19 working environment.

- The cyber resilience of the insurance sector is supported by many well-established national systems and initiatives, led by both government and industry, facilitating the sharing of incident information and best practises, among other things. At European level, the industry is also preparing for cross-sectoral legislation – the European Commission's Digital Operational Resilience Act (DORA) – *lex specialis* to the NIS Directive – and sector-specific supervisory guidelines from the European Insurance and Occupational Pensions Authority (EIOPA) focused on ICT and cyber resilience. In this regard, above all else, Insurance Europe wishes to stress the importance of alignment between the various initiatives from different authorities so that any multiplication of obligations and requirements on organisations, all of which may be intended at achieving the same goal (of increasing cyber resilience), can be avoided. In light of the many existing rules in force and many others in the pipeline,[1] close coordination between authorities in this area is essential. Otherwise, the regulatory environment to which organisations are subject becomes difficult to navigate, interfering with an organisation's ability to ensure a high level of cyber resilience and detracting from the added value of having such requirements in place.
- We note that Recitals 12, 13 and 14 of the NIS Directive recognise the high degree of harmonisation of financial supervision at EU level, and the advantages that this carries as regards supervision of operational risk. In this context, Insurance Europe would also like to draw attention to the question of human resources among the financial supervisors that are tasked with overseeing insurers' ICT security and compliance with rules. In order to effectively carry out their duties, it is vital that supervisors have the necessary skills and expertise to be able to do so, given that cybersecurity is a complex and ever-evolving area.
- In sum, Insurance Europe believes that the scope of the NIS Directive should **not** be extended to include the insurance industry – as to do so would be to introduce duplicate requirements. Furthermore, for obvious competition reasons and in the interests of achieving the Single Market objective of a level playing field, member states should not be allowed to go beyond the core sectors designated under the NIS Directive and include insurers in the scope, as Operator of Essential Services (OES). Rules governing insurers' cyber resilience should not be divided into many separate pieces of legislation or supervisory guidelines but should be governed only by the forthcoming DORA, complementing the many existing national initiatives.

Section 1 – General questions on the NIS Directive

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

[1]See future EIOPA's Guidelines on Information and Communication Technology security and governance, EIOPA's Guidelines on outsourcing to cloud service providers

Q1: to what extent are these objectives still relevant? (1-5: 1 is not relevant at all, 2 is not relevant, 3 is relevant, 4 is very relevant, 5 is don't know/no opinion)

- Increase the capabilities of Member States **5**
- Improve the level of cooperation amongst Member States **5**
- Promote a culture of cybersecurity across all sectors vital for our economy and society **5**

Additional comments:

Insurance Europe is not in a position to comment generally on the relevance of the objectives envisaged by the NIS Directive. In all but four member states, insurance is not considered as a critical sector, as, for the most part, the criticality of the services provided by insurance companies does not compare with those offered by the sectors identified by the directive. As regards the four countries that have included the insurance sector in the category of OES, not enough time has elapsed to allow for conclusions to be drawn on the effects of the Directive in terms of cyber resilience (most countries are only at the initial stages of implementing the Directive's requirements).

1.b – Cyber-threat landscape

Q1: Since the entry into force of the NIS Directive in 2016, how in your opinion has the cyber threat landscape evolved? (1-6: 1 is cyber threat landscape has decreased significantly, 2 is decreased, 3 is stayed the same, 4 is increased, 5 is increased significantly, 6 is don't know/no opinion)

- 4

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)

- 4

Additional comments:

- The level of preparedness of SMEs in the EU against current cyber threats varies from business to business. In the context of COVID-19, it is probably fair to assume that many SMEs were less prepared for the move to teleworking than larger companies, and may have had less resources at their disposal to invest in secure ICT infrastructure and VPNs for use alongside home networks, relying primarily on personal devices. However, specifically as regards insurance companies that fall into the category of SMEs, the experience of COVID-19 and, in particular, the lack of notable ICT incidents, has demonstrated that these companies were adequately prepared to adapt to the new teleworking conditions. This leads to the conclusion that insurance SMEs have a high level of ICT security, and that such stress situations are provided for in their business impact analyses.

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?

It is important that any EU cybersecurity policy is sufficiently high-level and principles-based in order to be adaptable to technological advances and trends. In this sense, it is also important that cybersecurity policy leaves room for businesses to innovate, while also balancing the need to ensure a level playing field in the Single Market. The development of AI and other new technology applications must also incorporate principles of cybersecurity 'by-design'.

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? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is 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: **5** (don't know/no opinion)
- 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: **3** (agree)
- All entities of a certain size providing essential services to our society should be subject to similar EU-wide cybersecurity requirements: **2** (disagree)

Additional comments:

- While it is too general a statement to say that "cybersecurity rules should be aligned at Union level", it may be appropriate for *high level principles* of cybersecurity to be aligned at Union level, as is foreseen under the soon-to-be published proposal for a DORA for the financial sector. Any legislation in this area should be sufficiently principles-based so as to be adaptable to the evolving nature of cyber risk, describing the objectives to be achieved rather than prescribing technical solutions. Importantly, alignment of rules should not apply to "all entities of a certain size" but should rather be risk-based; that is to say, in proportion to the risks faced by an entity and the services that need to be protected and maintained.

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.

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)
If yes, please specify which sectors, subsectors and/or digital services.

- While Insurance Europe is not in a position to comment on the broader inclusion of certain sectors/subsectors/digital services in the scope of the Directive, it firmly opposes extending the scope of the Directive to include the (re)insurance industry. The guiding principle for the inclusion (or not) of a sector in the scope of the NIS Directive should be its level of criticality for the functioning of the real economy. The criticality of those sectors currently provided for under the scope of the Directive (Banking, Energy etc.) – and the broader implications that an attack on their ICT systems would have for the economy and society – cannot, for the most part, be compared with that of the (re)insurance industry. For those services provided by insurers that *are* of a critical nature, experience of the COVID-19 pandemic has shown that they are adequately protected. Please refer to the additional comments (in annex) for a more detailed response.

Additional comments:

- As previously mentioned, the guiding principle for the inclusion (or not) of a sector in the scope of the NIS Directive should be its level of criticality for the functioning of the real economy: ie if a sector is of immediate importance for the daily functioning of the real economy, it should be included in the scope of the Directive. For example, the banking sector, as a provider of liquidity, has an essential role in the daily functioning of many businesses and citizens. By contrast, the insurance sector is not a sector providing many services which are of immediate importance for the daily functioning of the real economy. Although risk transfer to insurance carriers is important for many businesses and citizens, insurance services are usually not essential for their daily operations. In other words, if the activities of a bank would be interrupted for several hours, the functioning of thousands of companies would be directly and severely impacted, making these banking activities absolutely critical. However, if the insurance services of an insurance company would be interrupted for several hours or even days, this should not necessarily have far-reaching consequences for the functioning and daily operations of the companies and citizens who have bought these services.
  Furthermore, the experience of the COVID-19 pandemic has demonstrated that European insurers are well-developed in terms of their cyber preparedness and resilience. Since insurers transitioned to the new COVID-19 working environment, only one major cyber incident involving the industry has been reported, involving a large Spanish insurance company that fell victim to a cyberattack in August 2020. The company in question recovered 90 percent of its services within a very short timeframe, recovering 100 percent of its services soon afterwards. The speed and efficiency of this response demonstrates that the possibility of such an attack was already provided and prepared for in the company's business impact analysis. Thanks to this, the event resulted in minimal disruption of services to clients. There have been no other incidents reported – of any size or involving any profile of insurer – and, on the contrary, a survey conducted by one national insurance association has drawn the conclusion that the industry was well-positioned to respond to the ICT challenges brought on by the pandemic. In other words, the ICT security and contingency programmes put in place by European (re)insurers have proven to be robust when confronted with the new COVID-19 working environment.
  Moreover, although insurance services are becoming more digitalised, their provision does not depend exclusively on network and information services, since it is always possible to provide the service outside of the digital distribution channel, in the traditional face-to-face, physical model. In any case, it goes without saying that proper management of business interruption risks remains important for insurance companies and for this purpose appropriate prudential regulation is in place (ie Solvency II laws and regulations).

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?

- Cloud providers and providers of SAAS should be, at a minimum, subject to the same requirements as OES.

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)
If yes, please specify which types of information they should make available and to whom.

- No

Additional comments:

- Insurers currently under the scope of the Directive are not in favour of additional reporting requirements, but rather call for a clear and efficient framework that does not exceed the granularity of the reporting systems currently in existence at national level (see additional comments on Q2.f.1). An incident notification framework is provided for in the draft outline of the DORA proposal.
  In general terms, in the area of reporting, there is a risk of information overlap with different public authorities and institutions in charge of cybersecurity matters gathering information by themselves, leading to an excessive burden on companies. From a private sector point of view, it is therefore crucial that any complementary demand for information is coordinated between the different competent authorities. Furthermore, given that the overall aim of such initiatives is increased cyber resilience, organisations must benefit from sharing information with authorities and any mechanism must be reciprocal, allowing participating organisations to access anonymised and aggregated data in return for their participation.
  Lastly, for organisations that wish to participate, voluntary sharing of information on, for example, attempted intrusions and near misses, would allow for a better mapping of the threat landscape. This could be complemented by information on the types of measures preventing attacks, KPIs, etc.

Section 2 – Functioning of the NIS Directive

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? (1-5: 1 is not relevant at all, 5 is don't know/no opinion)

- 3 (relevant)

Additional comments:

- Common objectives at EU level could serve as good targets to help in identifying the strategy to be implemented at national level, taking into account the local context. However, common objectives should remain as such, leaving enough room to manoeuvre for organisations to be able to adapt their ICT practises to the evolving nature of the risk.

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)

- 5 (don't know/no opinion)

Additional comments:

- It is not possible to give a general answer to this question, as national strategies must take into account each national situation and individual national specificities.

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? (1-5: 1 is no impact, 2 is low impact, 3 is medium impact, 4 is high impact, 5 is don't know/no opinion)

	No impact	*Low impact*	*Medium impact*	*High impact*	*Don't know / no opinion*
Level of funding			**X**		
Level of staffing			**X**		
Level of expertise			**X**		
Cooperation of authorities across Member States				**X**	
Cooperation between national competent authorities within Member States				**X**	

Q2: In your opinion, what is the impact of the NIS Directive on national Computer Security Incident Response Teams (CSIRTs) in the Member States? (1-5: 1 is no impact, 2 is low impact, 3 is medium impact, 4 is high impact, 5 is don't know/no opinion)

	No impact	*Low impact*	*Medium impact*	*High impact*	*Don't know / no opinion*
Level of funding			**X**		
Level of staffing					**X**
Level of operational capabilities					**X**
Level of expertise					**X**
Cooperation with OES and DSP			**X**		
Cooperation with relevant national authorities (such as sectoral authorities				**X**	

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)

- 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)

- 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)

- No opinion

Q6: If you are an OES/DSP: Has your organisation received technical support from the national CSIRTs in case of an incident? If yes, please rate the usefulness of this support (yes, no, don't know/no opinion)

- No

Q7: Should the CSIRTs be assigned additional tasks so far not listed in the NIS Directive? If yes, please specify which tasks. (yes, no, don't know/no opinion)

- No

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)

- Cross-border cooperation with the relevant authorities in other Member States
- Cooperation with the Cooperation Group
- Cooperation with the CSIRTs network

- No opinion

Q9: Should the single points of contact be assigned additional tasks so far not listed in the NIS Directive? If yes, please specify which tasks. (yes, no, don't know/no opinion)

- No, the 13 tasks for which the cooperation group is responsible seems complete.

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)

- Don't know / no opinion

The level of consultation and cooperation follows the rules defined by the Directive: ie regular meetings in order to exchange best practices and experiences, and to exchange information on actors operating in several European countries.

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? (1-5: 1 is strongly disagree, 5 is don't know/no opinion)

	Strongly disagree	*Disagree*	*Agree*	*Strongly agree*	*Don't know / no opinion*
The current approach ensures that all relevant operators are identified across the Union.					**X**
OES are aware of their obligations under the NIS Directive.			**X**		
Competent authorities actively engage with OES.			**X**		
The cross-border consultation procedure in its current form is an effective element of the identification process to deal with crossborder dependencies.					**X**
The identification process has contributed to the creation of a level playing field for companies from the same sector across the Member States.					**X**

Additional comments:

- Rather than the identification process, it is the transposition of the NIS Directive that has not contributed to the creation of a level playing field for companies from the same sector across the member states. Because of the principle of minimum harmonization (see art. 3 of NIS Directive), the transposition processes in four member states have been very different than in the other 27 Member States – as far as insurers are concerned. For countries that have identified insurance companies as

an OES, it has involved the introduction of increased, detailed and costly requirements. There is therefore a necessity to align cybersecurity requirements at EU level, as foreseen under the DORA, rather than allowing individual member states to decide for themselves.

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? (1-5: 1 is strongly disagree, 5 is don't know/no opinion)

	Strongly disagree	*Disagree*	*Agree*	*Strongly agree*	*Don't know / no opinion*
Definitions of the types of entities listed in Annex II are sufficiently clear.				**X**	
More sectors and sub-sectors should be covered by the Directive.	**X**				
Competent authorities actively engage with OES.			**X**		
Identification thresholds used by Member States should be lower (i.e. more companies should be covered).	**X**				

- Regarding an extension of the scope of the Directive to cover more (sub)sectors (statement 2) and lowering the threshold for identifying companies (statement 3): while, in principle, Insurance Europe recognises that the growing dependence on ICT systems calls for a renewed focus on the security of these systems, the secretariat takes the view that, as regards the insurance industry, this is already provided for by a combination of national and European rules. Furthermore, the forthcoming European Commission proposal for a DORA for financial services is expected to apply to virtually all financial entities, rendering pointless an extension of the scope of the NIS Directive or a lowering of its thresholds.

Additional comments:

- While (re)insurers – over a certain criticality threshold – in only four member states are currently in the scope of the NIS Directive, there are many long-standing and well-functioning systems in place in other member states that function independent of the Directive.

  In Belgium, for example, the National Competent Authority (National Bank of Belgium - NBB), has not included insurance companies in the scope of the NIS Directive, however, the largest six Belgian insurance companies have been identified as systemically important financial institutions, and consequently, have been subjected to additional prudential requirements relating to the proper management of business interruption risks and business continuity. For this purpose, a dedicated circular with far-ranging requirements (ie " strategy, policy and risk analysis", based on international standards, "awareness-raising", "incident and problem management", "recovery and resumption objectives", "fall-back testing", etc) was published on the website of the NBB (cf. Circular NBB_2015_32 'Additional prudential expectations regarding operational business continuity and security of systemically important financial institutions'). These measures are considered appropriate as they are risk-based and do not affect all Belgian insurance companies equally, reflecting their different risk profiles. The success of the national-specific Belgian approach suggests that there is no need to extend the scope of the NIS Directive to include the insurance industry.

  Please refer to the additional comments on question 2.f. (Incident notification) for more examples.

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?

- N/A

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? (1-6: 1 is very significant decrease in risk, 5 is very significant increase in risk, 6 is don't know/no opinion)

	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			**X**			
Oil			**X**			
Gas			**X**			
Air transport				**X**		
Rail transport			**X**			
Water transport						
Road transport			**X**			
Banking				**X**		
Financial market infrastructures				**X**		
Health sector					**X**	
Drinking water supply and distribution			**X**			
Digital infrastructure (IXPs, DNS providers, TLD registries)			**X**			

Q5: How do you evaluate the level of cybersecurity resilience when it comes to the different sectors and subsectors covered by the NIS Directive? (1-6: 1 is very low, 5 is very high, 6 is don't know/no opinion)

	Very low	*Low*	*Medium*	*High*	*Very high*	*Don't know / no opinion*
Electricity		**X**				
Oil		**X**				
Gas		**X**				
Air transport		**X**				
Rail transport		**X**				
Water transport		**X**				
Road transport		**X**				
Banking				**X**		
Financial market infrastructures				**X**		
Health sector		**X**				
Drinking water supply and distribution		**X**				

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)

- **Small companies** (room to elaborate)

- **Medium-sized companies** (room to elaborate)

- As has been previously stated, the level of cyber resilience and the risk-management practises of insurance SMEs (not covered by the NIS Directive) is considered to be high. This assessment is supported by the experience of COVID-19, during which SMEs transitioned to teleworking without experiencing ICT-related incidents. Many insurance SMEs are located in Germany, where a survey was conducted assessing the experiences of companies, which detected no incidents and found that the industry was well-positioned to handle the crisis.

  Any new rules governing cyber resilience must take into account the principle of proportionality, as SMEs cannot meet the same requirements as large companies for organisational and technical reasons alone.

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)? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

	Strongly disagree	*Disagree*	*Agree*	*Strongly agree*	*Don't know / no opinion*
Annex III of the NIS Directive covers all relevant types of digital services		**X**			
Definitions of the types of digital services listed in Annex III are sufficiently clear.		**X**			
DSPs are aware of their obligations under the NIS Directive.			**X**		
Competent authorities have a good overview of the DSPs falling under their jurisdiction					**X**
Competent authorities actively engage with DSPs under their jurisdiction.					**X**
Security requirements for DSPs are sufficiently harmonised at EU level					**X**
Incident notification requirements for DSPs are sufficiently harmonised at EU level.					**X**
Reporting thresholds provided by the Implementing Regulation laying down requirements for Digital Service Providers under the NIS Directive are appropriate.					**X**

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?

- **All Internet Service Providers**

The Outsourcing:

- Outsourced application maintenance
- Third Applications Formula and testing: externalised management tests
- BPO: Business process Outsourcing

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)? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

	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			**X**		
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.					**X**
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.		**X**			
The exclusion of micro- and small enterprises is reasonable considering the limited impact of their services on the economy and society as a whole.			**X**		

Q4/5: How do you evaluate the level of preparedness of digital service providers covered by the NIS Directive when it comes to cybersecurity related risks? (1-6: 1 is very low, 5 is very high, 6 is don't know/no opinion)

	Very low	*Low*	*Medium*	*High*	*Very high*	*Don't know / no opinion*
Online marketplaces		**X**				
Online search engines				**X**		
Cloud computing services				**X**		

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? (1-6: 1 is very significant decrease in risk, 5 is very significant increase in risk, 6 is don't know/no opinion)

	Your elaboration
Online marketplaces	The security budget in the majority of companies remains low, especially for small compagnies.
Online search engines	The experiences of cyberattacks they have faced and the demand of companies that provide services to other companies makes them better prepared for cyberattacks. They are also required to carry out internal audits to reassure their customers.

Cloud computing services	The experiences of cyberattacks they have faced and the demand of companies that provide services to other companies makes them better prepared for cyberattacks. They are also required to carry out internal audits to reassure their customers.

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? (1-6: 1 is very low, 5 is very high, 6 is don't know/no opinion)

- **Online marketplaces**
- **Online search engines**
- **Cloud computing services**

- **Don't know/no opinion**

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? (1-5: 1 is no impact, 2 is low impact, 3 is medium impact, 4 is high impact, 5 is don't know/no opinion)

- The impact of imposing security requirements on OES depends entirely on the starting level of cyber resilience of the OES in question.

  In France, the introduction of security requirements on OES under the NIS Directive has had a significant impact in terms of cyber resilience, for example:
  - For essential Information Services, 23 rules were introduced by decree 14/08/2018[2].
  - Many OES managers have decided to invest in cybersecurity and not only for essential ICT, but for all ICT systems.
  - Many projects have been launched to avoid penalties, but also to ensure the resilience of the ICT system in case of a cyber attacki
  - Nevertheless, not enough time has passed to allow for conclusions to be drawn on the effects of these measures on the actual cyber resilience of OES (countries have only recently implemented the Directive).

Q2: What is the impact of imposing security requirements on DSPs by the NIS Directive in terms of cyber resilience? (1-5: 1 is no impact, 2 is low impact, 3 is medium impact, 4 is high impact, 5 is don't know/no opinion)

- High impact

Q3.a: To what extent do you agree with the following statements regarding the implementation of security requirements under the NIS Directive? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

	Strongly	*Disagree*	*Agree*	*Strongly*	*Don't know*

[2] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037444012

	disagree			*agree*	*/ no opinion*
Member States have established effective security requirements for OES on a national level.					**X**
There is a sufficient degree of alignment of security requirements for OES and DSPs in all MS.					**X**

Q3.b: Are there sectoral differences for OES regarding how effectively security requirements have been put in place by the Member States? If yes, please specify for which sectors and elaborate. (yes, no, don't know/no opinion)

- Don't know/no opinion

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? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

	Strongly disagree	*Disagree*	*Agree*	*Strongly agree*	*Don't know / no opinion*
Prescriptive requirements make it easy for companies to be compliant		**X**			
Prescriptive requirements leave too little flexibility to companies.				**X**	
Prescriptive requirements ensure a higher level of cybersecurity than general risk management obligations.		**X**			
Prescriptive requirements make it difficult to take into account technological progress, new approaches to doing cybersecurity and other developments.				**X**	
The different level of prescriptiveness of requirements increases a regulatory burden for companies operating across different national markets				**X**	
The companies should have the possibility to use certification to demonstrate compliance with the NIS security requirements.				**X**	
The companies should be required to use certification for their compliance with NIS security requirements.		**X**			

- Prescriptive requirements are not suited to the fast-evolving nature of cyber risk. Due to technological progress, prescriptive requirements tend to become quickly outdated, placing undue burden on the subjected companies. As such, in line with the evolving prudential requirements in the financial sector, a risk-based approach to cyber resilience – that draws on principles rather than imposing prescriptive requirements - is more favourable and will obtain the same outcomes. In the same vein, the use of certification schemes should not be a requirement but could be a means for companies to demonstrate that they have taken appropriate measures to contain risks within acceptable boundaries.

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? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

	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.		**X**			
Member States have imposed notification requirements obliging companies to report all significant incidents.					**X**
Different reporting thresholds and deadlines across the EU create unnecessary compliance burden for OES.					**X**
The current approach ensures that OES across the Union face sufficiently similar incident notification requirements.					**X**

- While, in general, the above statements do not apply to the insurance industry in the context of the NIS Directive, as far as the industry is concerned, there are many other existing mechanisms in place at member state level for incident notification and information exchange.

Additional comments:

- In Germany, while, in principle, (re)insurers over a certain criticality threshold have been designated as OES and are subject to requirements under the NIS Directive, companies of all sizes and risk profiles participate voluntarily in a national incident reporting system, the LKRZV (Crisis and Response Centre of the Insurance Industry). The LKRZV facilitates event-related communication for the purpose of early detection, alerting and management of crises, together with the Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik) and insurance companies on a 24/7 basis. The LKRZV is a two-way reporting and communication process, allowing not only pseudonymous reporting but also distributing information, alert and requests to the insurers in a coordinated, timely manner.

  Since 2017, the French government, along with the French Federation of Insurance and other stakeholders have created a public interest group, GIP ACYMA. This public-private partnership brings together private and public players who wish to get involved in the action of the Cybermalveillance.gouv.fr system which consists in active participation in working groups on targeted projects (eg prevention), in contributing to certification processes, but also in the setting up of a Digital Risk Observatory, a tool to support decision-making and public action. In addition, some (re)insurers in France are members of a cross-sectoral group, INTERCERT-FR, which is dedicated to strengthening the capacity of its members to detect and manage cyber security failures.

  Some (re)insurers in Denmark, Norway, Sweden and Iceland are members of the Nordic Financial CERT, established to strengthen the Nordic financial industry's resilience to cyberattacks, by enabling Nordic financial institutions to respond rapidly and efficiently to cyber security threats and online crime. As a collaborative initiative, it allows members to work together when handling cybercrime, sharing information and responding to threats in a coordinated manner.

  In the Netherlands, most insurance companies are connected to the Computer Emergency Response Team (i-CERT) of the Dutch Association of Insurers. This allows for real-time information sharing on cyber threats, incidents and vulnerabilities between Dutch insurance companies.

In Belgium, the insurance sector is involved in several initiatives to mitigate cyber risk. Notably, most Belgian insurance companies are connected to the so-called "Early warning system" that was established by Assuralia, the Belgian association of insurers, to facilitate real-time information sharing on cyber threats, incidents and vulnerabilities between Belgian insurance companies. Assuralia has also been a member of the Belgian Cyber Security Coalition since its foundation. The Coalition's objective is to bolster Belgium's cyber security resilience by building a strong cyber security ecosystem at national level, by bringing together the skills and expertise of academics, the private sector and public authorities on a trust-based platform aimed at fostering information exchange and implementing joint actions.

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? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion). Please elaborate your answers

	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.					**X**
The approach increases costs for OES operating in more than one Member State.			**X**		
The approach allows Member States to take into account national specificities.					**X**

- Once again, Insurance Europe can only react to the above statements in the context of its own industry, where certain (re)insurers in four MS fall in the scope of the Directive, while others do not. Differences in MS transposition do not, however, imply that security standards are weaker amongst insurance companies outside the scope of the Directive. As outlined in the additional comments on questions 2.c.2. and 2.f., MS have put in place many national-specific security practises independent of the NIS Directive.

Additional comments:

- As regards insurance companies designated as OES that operate cross-border, these are most likely to be large companies with sophisticated ICT risk management practises in place, based on internationally-recognised standards and frameworks such as the NIST Cybersecurity Framework and the ISO 27k series (see question 2.e.1).

  The uneven playing field that has resulted from the different ways that MS have transposed the Directive has generated difficulties for pan-European insurance companies, especially for subsidiaries of insurance groups that have been designated as OES.

  It is expected that the forthcoming proposal for a DORA for the financial sector will seek to fill any perceived gaps in existing financial sector-specific security requirements in place in member states.

Regarding costs, the implementation of micro-segmentation between the essential information system, its sub-systems and the rest of the information system (IS), and in particular the repositories, log reports, as well as audits and certification can be a major financial burden for companies.

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? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

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

Additional comments:

- In France, the regulation provides the following penalties for OES managers:
  - Failure to comply with security obligations: 100,000 euros
  - Failure to report an incident: 75,000 euros
  - Obstruction of control operations: 125,000 euros

- The German IT security act applicable at national level obliges operators of critical infrastructures to better protect their networks from cyber incidents. In addition to the mandatory reporting of IT security incidents, industries must develop their own standards, which will then be approved by the Federal Office for Information Security. This national law and the responsible supervisory authority effectively implement the requirements and are sufficient. The resulting interaction between the requirements of the security act and the supervisory authority is effective and does not require the introduction of further fines or other penalties.

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? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

	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					**X**
The Cooperation Group has played an important role in aligning national transposition measures					**X**
The Cooperation Group has been instrumental in dealing with general cybersecurity matters			**X**		
The Cooperation Group is dealing with crossborder dependencies in an effective manner.					**X**
The CSIRTs network has effectively managed to fulfil its tasks as laid down in the NIS Directive.					**X**
The CSIRTs network has helped to build confidence and trust amongst its members.			**X**		
The CSIRTs network has achieved swift and effective operational cooperation.					**X**
The Cooperation Group and the CSIRTs network cooperate effectively.					**X**

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.

- Don't know/no opinion

Q3: Should the CSIRTs network 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.

- Don't know/no opinion

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? (1-5: 1 is not at all, 2 is to a little extent, 3 is to some extent, 4 is to a large extent, 5 is don't know/no opinion)

- 3

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? (1-5: 1 is no impact, 2 is low impact, 3 is medium impact, 4 is high impact, 5 is don't know/no opinion)

- As regards the fur countries that have included the insurance sector in the category of OES, not enough time has elapsed to allow for conclusions to be drawn on the effects of the Directive in terms of cyber resilience (most countries are only at the initial stages of implementing the Directive's requirements).

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? (1-5/don't know/no opinion)

- No coherence: The provisions of the NIS Directive overlap with certain planned requirements for financial institutions under a future DORA framework, on which a Commission proposal is expected in Q3 of this year. It is important that there is alignment between the various initiatives from different authorities so that any multiplication of obligations and requirements on organisations, all of which may be intended at achieving the same goal (of increased cybersecurity), can be avoided. Otherwise, the regulatory environment to which organisations are subject becomes difficult to navigate, and so interferes with an organisation's ability to ensure compliance and detracts from the added value of having such requirements in place.

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

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?

- Organisations could be incentivised to share more information with cybersecurity authorities on a voluntary basis if their participation gave them reciprocal access to the anonymised and aggregated data on cyber incidents reported by other organisations. The availability of such data, as part of a two-way voluntary reporting system, would allow public institutions to better understand the threat landscape and would assist private organisations in preparing for and responding to future threats. To make such a mechanism increasingly efficient, it would be important to avoid the multiplication of authorities to which financial institutions report incidents. Lastly, the participation of insurance companies could be incentivised by allowing them to make use of the incident data for underwriting purposes, encouraging the growth of the European cyber insurance market and contributing to the overall cybersecurity of businesses.

Q2.a: 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)

- No

Q2.b: If yes, to which other types of information should the reporting obligations be broadened?

- See response to 1g and 2f.

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.)?

- Given the cross-border nature of cyber incidents, the EU has a role to play in supporting and promoting the exchange of information between the relevant authorities of the Member States and also between companies. Strengthening the cross-border response teams can lead to faster and better action in the area of countermeasures. An increased exchange of information at European level is therefore welcomed. Shared data, once anonymized and aggregated, could contribute to strengthening the cybersecurity of businesses across the EU. Lastly, for organisations that wish to participate, voluntary sharing of information on, for example, attempted intrusions and near misses, would allow for a better mapping of the threat landscape. This could be complemented by information on the types of measures preventing attacks, KPIs, etc.

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.

Q2: How would you evaluate the level of information exchange between organisations across sectors when it comes to cybersecurity? (1-6: 1 is very low level, 5 is very high level, 6 is don't know/no opinion)

- Please refer to the additional comments in response to question 2.f. (Incident notification).

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

- When looking to improve the level of information exchange, there are several challenges that need to be addressed. One of the major impediments to cross-sectoral and cross-border information exchange is the associated reputational issues, since this information could affect an organisation's relationship both with its supervisor and with its peers. It is therefore of the utmost importance that any system of information exchange is either anonymous or pseudonymous. Other impediments to establishing such systems include the degree of fragmentation of both information collecting and information sharing practises, both across different sectors and across different jurisdictions, and the lack of a common taxonomy on cyber risk (definitions, thresholds) which may complicate the development of streamlined templates for information exchange. In any event, trans-sectoral working groups exchanging on feedback/experience/best practices could be useful.

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? (1-6: 1 is very low level, 5 is very high level, 6 is don't know/no opinion)

- Don't know/no opinion

Q2: Have you implemented a coordinated vulnerability disclosure policy? (yes, no, don't know/no opinion, not applicable)

- Not applicable

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

- Known vulnerabilities should be explored under the aegis of the risk of the threat occurrence.

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

- Yes

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)

- Yes

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? (1-5: 1 is strongly disagree, 4 is strongly agree, 5 is don't know/no opinion)

	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.					**X**
European legislation should require Member States to put in place frameworks to raise awareness amongst SMEs and support them.			**X**		

- In Germany, the LKRZV, which has already been explained in detail in response to other questions, offers support to SMEs.
- In France, as mentioned before, the GIP ACYMA carries out three main tasks:
  - Assisting victims of cyber-attacks.
  - Informing and raising awareness about digital security.
  - Observing and anticipating digital risk.