Insurance Europe response to the consultation on the revision of the Cybersecurity Act

Our reference:	EXCO-CS-25-025	Date:	20-06-2025
Referring to:	EC consultation on revising the EU Cybersecurity Act		
Contact person:	Alana Fitzpatrick, Policy Advisor	E-mail:	Fitzpatrick@insuranceeurope.eu
Pages:	17	Transparency Register ID no.:	33213703459-54

Insurance Europe welcomes simplification in the area of digital regulation as an opportunity to reduce the regulatory and administrative compliance burden on companies. The revision of the Cybersecurity Act and the upcoming digital simplification omnibus provides such opportunity to ensure that the various digital regulations are pragmatic and risk-based. The insurance industry would welcome the reduction of overlaps and duplications in cybersecurity reporting and the involvement of industry stakeholders in developments towards certification.

Simplify cybersecurity reporting burdens

Recent EU legislations have focused on strengthening cybersecurity measures across the Union, focusing on tackling third-party ICT risk, mandating cyber reporting and a renewed focus on testing to increase cyber resilience. Insurers are primarily subjected to the Digital Operational Resilience Act (DORA) as a key sector-specific legislation for the financial sector, however horizontal legislation also applies such as the GDPR, the e-Privacy Directive, the AI act and in some instances, the Cyber Resilience Act. The DORA measures are complex and burdensome to implement, which companies have invested in heavily over the past years ahead of the January 2025 application date. With new cyber reporting introduced, this has led to a duplication of reporting of cyber and data incidents under different pieces of legislation, according to different timelines, as well as reporting to multiple national agencies in some jurisdictions.

Measures to reduce and streamline the reporting burden to avoid unnecessary duplication would be welcomed. Particularly, aligning cyber reporting mechanisms under different pieces of legislation and centralising the notifications would help companies to not repeat submissions of notifications. It should also be ensured that across various jurisdictions, the reporting formats are comparable to not complicate the process and to avoid creating differing interpretations to reporting requirements. For instance, clarifying the interplay of the DORA and Solvency II texts regarding the reporting of third-party risk would be welcome.

The increased focus on cybersecurity across the Union has also led to new or empowered national cyber agencies. Whilst this renewed guidance is welcome, in some countries there has been a duplication of cyber notifications to both the DORA supervisor (usually a financial service-related body, such as a central bank) and the cyber agency. This creates extra burdens for companies required to duplicate reporting. Better centralisation of reporting notifications would help to avoid this unnecessary duplication. For example, in Spain a new global resilience scheme for critical entities is being created that includes cyber resilience and could overlap with some of the already regulated elements in DORA, such as event notification. Further guidance from the EU to member states, to avoid these duplications which creates burden for companies, would be welcomed.

With regards to the list of digital regulations and guidelines, there is a need to ensure clarity on the applicable rules harmonised across the different jurisdictions. There are guidelines which have been replaced by specific legislation, however there are areas where overlapping rules are still in application. This is the case for instance in Ireland, where Guidelines Outsourcing to Cloud Service Providers (via the Central Bank of Ireland's own cross-sectoral guidance) are still in place whilst these were superseded by the EU-wide DORA regulation. It is important that there is legal and supervisory clarity across the Union.

European cybersecurity certification

Certification should be pursued mindfully to factor in that certification in itself can be an additional burden and cost for companies. In all situations, certification should remain a voluntary scheme as attempts to make it mandatory in the area of digital policies would have negative effects on companies' operations.

For future activities in the area of certification, greater transparency and more opportunities for stakeholder participation throughout the process are needed. Widespread concerns were raised by stakeholders on the European Cybersecurity Certification Scheme for Cloud Services (EUCS) in the past over the inclusion of political and sovereignty requirements within a technical scheme intended to develop cybersecurity standards.

The lack of transparency in the process and limited opportunity for formal industry feedback during the drafting of the scheme was a major concern to the industry. The one and only public consultation carried out on the draft certification scheme took place in 2021, long before the introduction of sovereignty requirements that had not featured as part of the consulted version. The text underwent significant changes since the consultation took place and those changes were never made publicly available, undermining the trust in the process and the purpose of the requirements of the scheme.

It should be stressed that any introduction of sovereignty requirements that effectively limit the ability of insurers to choose between different service providers could have significant adverse implications for innovation, competition, cybersecurity and digital transformation capabilities in the sector. This would likely increase the costs incurred by European insurers in adopting cloud services, make insurers less agile and significantly disrupt their ability to scale cloud resources up or down to respond to fluctuating computing demands or to keep pace with customer needs. While there is clearly merit in further exploring the possibility of enhancing Europe's digital sovereignty, this should be a longer-term, political discussion at the appropriate EU level. A cybersecurity certification scheme that lacks sufficient opportunity for stakeholder involvement is not the appropriate mechanism by which to introduce such a policy.

Moreover, if the intention of this review of the Cybersecurity Act is to also consider potential changes to the mandate of ENISA, which may result in conferring greater responsibilities and tasks upon ENISA, it is even more crucial to ensure that greater transparency is enshrined in its working processes and that increased opportunities for stakeholder involvement are guaranteed.

The insurance industry stands ready to participate in future discussions on certification and simplification, to support European industry competitiveness.

Insurance Europe is the European insurance and reinsurance federation. Through its 39 member bodies — the national insurance associations — it represents insurance and reinsurance undertakings active in Europe and advocates for policies and conditions that support the sector in delivering value to individuals, businesses, and the broader economy.

insurance
europe

Annex: Insurance Europe response to questionnaire on the Cybersecurity Act revision consultation (via EU Survey)

Section 1: General questions on ENISA mandate

This section aims to introduce some general questions concerning the mandate of the European Union Agency for Cybersecurity (ENISA). The questions intend to gather information for the potential changes of the mandate and prioritization of tasks of ENISA, based on the related added value for stakeholders. The questions do not aim to assess ENISA's performance, which was subject to a previous evaluation exercise.

❖ **Current tasks of ENISA**

Q1. Please provide your views regarding the importance of each of the current cybersecurity tasks entrusted to ENISA:

ENISA's task	Very important	Important	Somewhat important	Not very important	Do not know / No opinion
***Development and implementation of Union policy and law** (e.g., assisting Member States to implement Union policy and law, assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies, etc.)		**X**			
***Building cybersecurity capacity** (e.g., assisting in activities aiming at bolstering cybersecurity across the EU, etc.)		**X**			
***Operational cooperation at Union level** (e.g., ENISA support for operational cooperation among Member States, EUIBAs and stakeholders, providing the secretariat of CSIRTs, assisting at the request of one or more Member States, in the assessment of incidents, etc.)	**X**				
***Market, cybersecurity certification, and standardisation** (e.g., support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes – monitoring developments, preparing candidate schemes, evaluating adopted schemes, standardisation and performing analyses of the main trends in the cybersecurity market, etc.)		**X**			
***Knowledge and information** (e.g., perform analyses of emerging technologies, perform long-term strategic analyses of cyber threats and incidents, collect and analyse publicly available information about incidents, etc.)	**X**				
***Awareness-raising and education** (e.g., raise public awareness of cybersecurity risks, organise regular outreach campaigns, promote cybersecurity education, etc.)	**X**				

ENISA’s task	Very important	Important	Somewhat important	Not very important	Do not know / No opinion
***Research and innovation** (e.g., contribute to the strategic research and innovation agenda)	**X**				
***International cooperation** (e.g., contribute to the implementation of the Union’s efforts when cooperating with third countries)	**X**				

❖ Section 1.a. ENISA providing support in policy implementation

The following subsection aims to analyse a core task of the Agency, namely the support in cybersecurity policy implementation.

Q1. Where do you see the biggest added value of ENISA in the following suggestions:

ENISA’s added value	Very important	Important	Somewhat important	Not very important	Do not know / No opinion
***Assisting Member States** to implement Union policy and law regarding cybersecurity consistently. Examples include: issuing opinions and guidelines, providing advice and best practices on topics such as the European Cybersecurity Certification Framework, risk management, incident reporting and information sharing, etc.		**X**			
***Assisting the Commission** with evidence-based information on the development and review of Union policy in the area of cybersecurity.	**X**				
***Support to industry (entities)** in the form of best practices and technical guidance through reports/studies and analysis.		**X**			
*ENISA’s contribution to the Union’s efforts to **cooperate with key international partners.**		**X**			

Q2. Do you see any other areas than those mentioned in Q1, where ENISA could bring big added value?

Please, elaborate (with maximum 100 words):

There are several areas for further involvement of ENISA:

- Supporting alignment with the FSB FIRE and standardisation of ICT reporting;
- Driving standards and dialogue across industries for cybersecurity;
- Ensuring effective liaisons with the European/ NATO Cyber Defence Agenda and industry.

However, guidance and instructions must not become mandatory cross-sector/sector-specific standards; instead, operators must be able to consider sector- and company-specific risk-based solutions.

❖ Section 1.b. ENISA providing technical support

Following the adoption of legislative acts such as the NIS2 Directive, Cyber Resilience Act, Cyber Solidarity Act, eIDAS Regulation on electronic identity and trust services, ENISA has received more specific technical tasks (establishing platforms, databases, templates, etc.) to support stakeholders in the implementation of EU law. ENISA will also establish a European Cybersecurity Support Centre for hospitals and healthcare providers, *as set out in the recent Action Plan on the cybersecurity of hospitals and healthcare providers. This sub-section of the survey aims to gather more information on how the mandate of the Agency could address this set of specific services and their priority for stakeholders.*

Q1. Do you consider that there should be additional technical tasks (apart from those included in the adopted legislative acts) that should be integrated in ENISA's mandate?

	Yes	*If yes, please provide some examples:*
	No	
X	Do not know/ no opinion	

Q2. Do you consider that ENISA is performing well in providing technical tasks (e.g. maintenance of platforms, databases and tools)?

	Yes
	No
X	Do not know/ no opinion

❖ Section 1.c. ENISA's collaboration with other bodies

The cybersecurity ecosystem has evolved significantly since the last revision of ENISA's mandate in 2019. New actors are now part of the cyber fora and the relationship of the Agency with other stakeholders has evolved. This sub-section of the questionnaire aims to gather stakeholder views on ENISA's eventual involvement with other bodies.

Q1. Do you consider that ENISA's relationship and/or its partnership with other EU agencies, bodies, institutions etc. should be better specified in the founding act (the Cybersecurity Act)?

	Strongly agree
X	Agree
	Disagree
	Strongly disagree
	Do not know/ no opinion

❖ Section 1.d. ENISA's support in situational awareness

The following subsection aims to analyse a core task of the Agency, namely the support of ENISA in operational cooperation and gather stakeholders' views on operational cooperation and the situational awareness picture.

Q1: Pursuant to the current Article 7 of the Cybersecurity Act, ENISA supports the operational cooperation at Union level by creating synergies with other Union entities, organising cybersecurity exercises, contributing to a cooperative response to large-scale cyber incidents by providing a secretariat role for the CSIRTs Network and, within its framework, supporting Member States in capacity building, information sharing, analysis of vulnerabilities and incidents and, upon request, providing support in relation to ex post technical inquiries regarding significant incidents.

In which areas defined in Article 7 should ENISA further strengthen its role? Which tasks, roles are no longer relevant? What new tasks, roles are important for ENISA to cover in the new mandate?

Please elaborate (with maximum 500 words):

/

Q2: Should ENISA's role in supporting the constituency with capacity building be further strengthened (i.e. with specific support for ransomware prevention; sector specific support offered by ENISA; exercises organised by ENISA; challenges organised by ENISA)?

X	Yes
	No
	Do not know/ no opinion

Q3: Do you think ENISA has a role to play in building a shared EU situational awareness picture together with other Union entities by providing relevant technical information?

X	Yes
	No
	Do not know/ no opinion

Please elaborate (with max 100 words):

Sharing information of current cyberattack vectors is crucial to enhance Europe's cyber resilience. However, incident reporting will only contribute to this goal if the information reported is analysed by a public authority and incorporated into a daily cybersecurity situation picture.

❖ Section 1.e. ENISA and skills and awareness

The following subsection aims to analyse a core task of the Agency, namely the assistance of ENISA in awareness-raising and education, focusing more specifically on cyber skills.

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

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
*ENISA **should continue developing the European Cybersecurity Skills Framework** (ECSF)			X		
*ENISA **should continue to coordinate EU-wide cyber awareness campaigns and challenges** (e.g. European Cybersecurity Month, the European Cybersecurity Challenge...) and to develop guidance and tools addressing cybersecurity education and cybersecurity awareness (e.g. AR-in-a-Box, CyberEducation Platform, Cybersecurity Education Maturity Assessment, training material...)			X		
*ENISA **should continue leading the work on developing an attestation scheme for cybersecurity skills**, allowing ultimately for quality assurance and recognition of certifications in cybersecurity					X

Section 2: Certification

This section is designed to explore key questions related to the European Cybersecurity Certification Framework (ECCF). The ECCF has a major role in strengthening cybersecurity to protect our industries, citizens and critical infrastructure against internal and external threats. Nevertheless, the evaluation of the Cybersecurity Act (CSA) has highlighted areas where improvements are needed, in particular as regards the adoption and governance process, the roles and responsibilities of the Member States, Commission and ENISA and the formalisation of the maintenance phase of the European cybersecurity certification schemes. Consequently, the questions in this section aim to collect insights to inform potential amendments to the ECCF, ensuring greater clarity, efficiency and stakeholder involvement.

❖ Section 2.a. Scope, objectives, elements of schemes and harmonisation principle

Q1. What are the considerations, if any, that would encourage you to apply for a certificate under the European cybersecurity certification scheme?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
*Certification as means to improve the security of products or services			**X**		
*Regulatory compliance, including presumption of conformity			**X**		
*International market access based on mutual recognition			**X**		
*Reduction of legal exposure and potential financial liabilities			**X**		
*Market or contractually required compliance			**X**		
*Customer trust and credibility			**X**		
*Reduction of administrative costs		**X**			

Please elaborate your answer and list other considerations that would encourage you to apply for a certificate (with maximum 200 words):

Security certifications must not lead to operators being forced to use the certified products. Feasibility, competitive issues, and implementation costs should also be considered.

Q2. What technologies / services or other related aspects would benefit from European cybersecurity certification in the next 5 to 10 years (e.g. IoT, crypto, PQC, physical security)?

Please elaborate your answer (with maximum 100 words):

IoT, crypto, PQC (Post Quantum Cryptography), AI/ML and Critical infrastructures (e.g. telecommunications, etc.)

Q3. Do you consider that the scope, objectives and elements of the ECCF as expressed in the current CSA are clearly defined?

	Strongly agree
X	Agree
	Disagree
	Strongly disagree
	Do not know/ no opinion

Please, elaborate your answer (with maximum 100 words):

/

Q4. Are there any elements that the European cybersecurity certification schemes should cover in addition to those currently foreseen in Article 54 of the Cybersecurity Act (i.e. assurance levels covered, evaluation criteria, vulnerability handling, content and format of certificates)?

Please elaborate your answer (with maximum 100 words):

/

Q5. Do you think there are elements of the European cybersecurity certification schemes that could and should be harmonised for all European cybersecurity certification schemes (i.e. vulnerability handling, peer review mechanism, mark and label, scheme maintenance)?

X	Yes	*If yes, please elaborate on your answer (max 100 words):* Standardisation could be implemented across the board to enhance transparency.
	No	
	Do not know/ no opinion	

Q6. Do you think European cybersecurity certification should be made mandatory for certain products / services / processes / managed security services?

	Yes	*If yes, please elaborate on your answer (max 100 words):*
X	No	
	Do not know/ no opinion	

Q7. Do you see a benefit in European cybersecurity certification that would be tailormade to specific use-cases (products / services for specific industries)?

	Yes	*If yes, please elaborate on your answer (max 100 words):*
	No	
X	Do not know/ no opinion	

Q8: Do you see a benefit in incorporating personal data protection requirements in European cybersecurity certification to ensure synergy with data protection certifications under the General Data Protection Regulation (GDPR)?

	Yes
	No
X	Do not know/ no opinion

Q9. To what extent do other recent EU legislations aimed at increasing the level of security of ICT products, ICT services and ICT processes, such as the Cyber Resilience Act or the NIS2 Directive, impact the ECCF?

On a scale from 1 to 5 with 5 indicating to the very highest extent

X					
0	*1*	*2*	*3*	*4*	*5*
Don't know/ no opinion					*To the very highest extent*

Please, elaborate your answer (with maximum 100 words):

/

Q10. Do you consider it useful to develop voluntary certification of entities that would support compliance with multiple cybersecurity and data security requirements of EU legislation (e.g. NIS2 Directive, DORA)?

On a scale from 1 to 5, with 5 indicating very useful

					X
0	*1*	*2*	*3*	*4*	*5*
Don't know/ no opinion					*Very useful*

❖ Section 2.b. Process of development and adoption of certification schemes

The following subsection aims to analyse the effectiveness, efficiency and transparency of the preparation and development of European cybersecurity certification schemes for ICT products, ICT services, ICT processes and managed security services in the Union for improving the functioning of the internal market.

Q1. Do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
*The time needed to develop and adopt a European cybersecurity certification scheme is satisfactory.					**X**
*European cybersecurity certification schemes need to be regularly updated and amended.		**X**			
*The process for the request, development and adoption of European cybersecurity certification schemes would benefit from increased transparency.					**X**
*The Union Rolling Work Programme is an effective way of ensuring that industry, national authorities and standardisation bodies prepare in advance for the future European cybersecurity certification scheme(s).					**X**

❖ Section 2.c. Governance of the certification framework

The questions in this subsection seek to gather views on potential changes to ENISA's mandate and prioritisation of its tasks within the ECCF including, but not limited to, preparation, development and maintenance of European cybersecurity certification schemes, thereby contributing to clarification of the roles and responsibilities.

Q1. What role do you consider ENISA should play in the following areas of the ECCF?

Statement	No role	Supporting role	Leading role	Do not know / No opinion
*Preparation / development of candidate schemes				**X**
*Maintenance of schemes: drafting of technical specifications				**X**
*Maintenance of schemes: organisation of ECCG subgroup meetings				**X**
*Guidance for application of schemes				**X**
*Promotion of the uptake of schemes				**X**
*Peer review mechanism				**X**
*Issuance of certificates for European cybersecurity certification schemes				**X**
*Testing and evaluation				**X**
*Presumption of conformity with EU legislation				**X**

You may elaborate your answer(s) in the table (with maximum 100 words):

/

❖ Section 2.d. Stakeholder involvement

The questions in this subsection aim to collect additional insights to inform potential amendments to the framework to ensure greater and more streamlined stakeholder involvement, particularly in the preparatory, development and maintenance phases of European cybersecurity certification schemes.

Q1. Do you represent or have you in the past represented an organisation in the European Cybersecurity Certification Group (ECCG)?

	Yes
X	No
	Do not know/ no opinion

Q2. How do you assess the level of effectiveness of the European Cybersecurity Certification Group?

	Very low effectiveness
	Low effectiveness
	Medium effectiveness
	High effectiveness
	Very high effectiveness
X	Do not know/ no opinion

Q3. To what extent do you agree with the following statements regarding the ECCG?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
*The ECCG and the ECCF would benefit from more organised stakeholder interactions during preparatory stages of cybersecurity certification schemes.				**X**	
*The role and tasks of the ECCG in the Cybersecurity Act are sufficiently clear.					**X**
*The ECCG has provided sufficient support to the Member States in the implementation of the ECCF.					**X**
*Member States should play a more active role in the governance of ECCG subgroups.				**X**	

Q4: Do you consider that the mandate of the ECCG should encompass additional tasks to those currently foreseen in the Cybersecurity Act?

The Cybersecurity Act outlines the tasks of the ECCG in Article 62(4), most prominently to advise and assist the Commission in its work to ensure the consistent implementation and application of the Title III of the Act.

	Yes	*If yes, please specify which tasks (max 100 words):*
	No	
X	Do not know/ no opinion	

Q5. In your view, to what extent are relevant stakeholders sufficiently involved in the development of European cybersecurity certification schemes?

X	Not at all
	To a little extent
	To some extent
	To a high extent
	Do not know/ no opinion

Q6. What other measures could be taken to further facilitate relevant stakeholders' participation?

Please, elaborate (with maximum 100 words):

Greater transparency and more opportunities for stakeholder participation throughout the process are needed. Widespread concerns were raised by stakeholders over the inclusion of political and sovereignty requirements in the draft EUCS, a technical scheme to develop cybersecurity certification standards. The lack of transparency in the process and limited opportunity for formal industry feedback during the drafting of the scheme was a major concern. The one and only public consultation took place in 2021, before the introduction of sovereignty requirements was even considered. Such changes were also never made publicly available, undermining stakeholder trust in the entire process.

Q7. Is your organisation directly or indirectly (through association) part of the Stakeholder Cybersecurity Certification Group (SCCG)?

	Yes
X	No
	Do not know/ no opinion

Q8. To what extent do you agree with the following statements regarding the SCCG?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
*****The SCCG has sufficient opportunities to participate in ECCF.					**X**
*****The SCCG actively contributes to the development of European cybersecurity certification schemes.					**X**
*****A single forum and governance mechanism with regular interactions with the ECCG, ENISA and the Commission could provide better opportunity for the group to fulfil its advisory role.					**X**

❖ Section 2.e. Supply chain security

Supply chain attacks have been identified as one of the seven prime cybersecurity threats by the ENISA Threat Landscape 2024 report and cybersecurity risks associated with ICT supply chains have been justifiably given a lot of attention in recent years. The EU has taken multiple legislative initiatives to address supply chain security. In particular, Title III of the Cybersecurity Act sets out a framework for the development and adoption of the European cybersecurity certification schemes which provide assurance of the cybersecurity level of ICT products, services or processes that are used in the ICT supply chains. The Directive (EU) 2022/2555 provides for an obligation on Member States to ensure that essential and important entities take *appropriate and proportionate technical, operational and organisational measures to manage the risks. Such measures should cover supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. The recently adopted Cyber Resilience Act introduces mandatory cybersecurity requirements for manufacturers and retailers to be met during the entire lifecycle of their products and at every stage of the supply chain.*

Q1. In your view, during the last five years, how has the level of risk of cybersecurity incidents originating from ICT supply chains of entities operating in critical and highly critical sectors evolved?

	Risk level has decreased significantly
	Risk level has decreased
	Risk level is the same
	Risk level has increased
X	Risk level has increased significantly
	Don't know / no opinion

Q2: In your opinion what were the most common types of threats that led to ICT supply chain related cybersecurity incidents?

Please, elaborate with maximum 100 words:

Common threats include ransomware, social engineering, tampering with software updates, compromise of third-party vendors, infiltration of continuous integration and deployment and threats from state-sponsored actors.

Q3. In your opinion, which sectors were the most affected by ICT supply chain incidents (please chose maximum 3)?

Between 1 and 3 selections

	Energy
	Transport
	Banking
	Financial markets infrastructures
	Health
	Drinking water
	Waste water
	Digital infrastructure
X	ICT service management (managed security services)
	Public administration
	Space
	Postal and courier service
	Waste management
	Manufacture, production and distribution of chemicals
	Production, processing and distribution of food
	Manufacturing
X	Digital providers
	Research

The Cybersecurity Act aims at achieving a high level of cybersecurity, cyber-resilience and trust within the Union, for which it addresses threats and risks related to network and information systems. Beyond technical factors, cybersecurity risks for ICT supply chains may also relate to non-technical factors such as undue influence by a third country on supplier (through for instance a strong link between the supplier and a government of a given third country, the third country's legislation, the supplier's corporate ownership or the ability for the third country to exercise any form of pressure on supplier). Such non-technical factors could pose unprecedented security challenges related to ICT supply chains that are currently not covered by the scope of the Cybersecurity Act.

Q4. Do you consider that there is a need to develop tools to address non-technical risks related to ICT supply chain security?

	Strongly agree
X	Agree
	Disagree
	Strongly disagree
	Do not know/ no opinion

You may elaborate your answer (with maximum 100 words):

Yes. Non-technical risks, such as jurisdictional exposure and geopolitical dependencies, can impact ICT supply chain resilience. These could be better integrated into third-party risk management (TPRM) frameworks. Developing clear, consistent tools or criteria would help organisations assess and address such risks alongside technical ones. However, any restrictions on the ability to freely choose providers should be avoided.

Q5. To what extent do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
*The application of organisational policies, processes and practices, including i.e. information sharing and vulnerability disclosure, in the area of cybersecurity risk management sufficiently mitigates all relevant risks related to the ICT supply chain security of entities.			X		
*Purely technical measures, such as the use of on-device processing, appropriate cryptography and other, can sufficiently mitigate all relevant risks related to the ICT supply chain security of hardware and software products.		X			
*The current European cybersecurity certification framework is an effective tool to facilitate cybersecurity safeguards for the public procurement of ICT products, ICT services and ICT processes.			X		

Section 3: Simplification

This section aims to gather stakeholders' views as regards simplification of the cybersecurity legislation in line with the Commission's simplification agenda. It gathers the stakeholders' views as to whether incident reporting requirements and cybersecurity risk-management could potentially benefit from further simplification and streamlining, with the intended benefit of reducing unnecessary administrative burden.

Q1. Which of the following EU pieces of legislation are/will be applicable to your entity/authority:

Select all that apply

X	Directive (EU) 2022/2555 (Network and Information Security Directive – **NIS2**)
X	Regulation (EU) 2022/2554 (Digital Operational Resilience Act – **DORA**)
X	Regulation (EU) 2024/2847 (Cyber Resilience Act – **CRA**)
	Directive (EU) 2022/2557 (Critical Entities Resilience Directive – **CER**)

X	Regulation (EU) 2016/679 (General Data Protection Regulation – **GDPR**)
X	Directive 2002/58/EC, as amended by Directive 2009/136/EC (**e-privacy Directive**)
	Commission Delegated Regulation (EU) 2024/1366 (Network Code on cybersecurity of cross-border electricity flows – **NCCS**)
	Aviation rules (Regulations (EC) No 300/2008 and (EU) 2018/1139 and the relevant delegated and implementing acts adopted pursuant to those Regulations)
X	Regulation (EU) 2024/1689 (**AI Act**)
	Other: please specify (max 100 words):

Q2. Which of the following cybersecurity-related requirements laid down in the EU legislation referred to in Q1 ("relevant EU legislation") create or are likely to create in the near future the biggest regulatory burden?

Please rate from 1 as the lowest burden to 6 as the highest burden

Different NIS2 incident reporting templates' formats, contents and procedures across the different EU Member States:

					X
1	*2*	*3*	*4*	*5*	*6*
Lowest burden					*Highest burden*

Different incident reporting tools/processes for relevant EU legislation at a national level:

			X		
1	*2*	*3*	*4*	*5*	*6*
Lowest burden					*Highest burden*

Different incident reporting thresholds defining a reportable/significant/severe incident under the NIS2 Directive and across the different relevant EU legislations:

					X
1	*2*	*3*	*4*	*5*	*6*
Lowest burden					*Highest burden*

Implementation of cybersecurity risk-management measures stemming from relevant EU legislation:

					X
1	*2*	*3*	*4*	*5*	*6*
Lowest burden					*Highest burden*

Overlap of cybersecurity risk-management measures stemming from relevant EU legislation:

			X		
1	*2*	*3*	*4*	*5*	*6*
Lowest burden					*Highest burden*

Requirements on how to prove implementation of cybersecurity risk-management measures ('compliance') stemming from relevant EU legislation:

				X	
1	*2*	*3*	*4*	*5*	*6*
Lowest burden					*Highest burden*

Please explain and if possible, provide a quantification to the burden (with maximum 100 words):

Variations in thresholds and reporting formats across member states can create challenges for organisations operating in multiple jurisdictions, potentially affecting the timeliness and coordination of incident response.

Requirements following DORA, especially compliance requirements regarding the ROI, are very burdensome for the companies and not proportionate enough to the risk profiles of companies in the insurance industry.

Differing regulation means that separate processes must be run, increasing costs of operations and also potentially delaying critical response time e.g. separate reporting for incidents diverting key staff from resolving the incident.

Q3. Do you consider that there are any other cybersecurity-related requirements laid down in relevant EU legislation not mentioned above that could be further streamlined?

X	Yes	*If yes, please elaborate on your answer (max 100 words):* /
	No	
	Do not know/ no opinion	

Q4. How effective do you consider the following solutions would be in removing administrative burden?

Please rate from 1 as the least effective to 6 as the most effective

Align reporting templates for NIS2 incident reporting of entities across all Member States:

					X
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Align reporting timelines for incident reporting across relevant EU legislation:

					X
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Align reporting requirements as regards content of reporting obligations across relevant EU legislation:

				X	
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce machine-readable standardised data formats for reporting across the EU:

					X
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce one comprehensive set of rules for incident reporting in EU legislation:

					X
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce a single reporting platform at national level for the compliance with reporting obligations stemming from relevant EU legislation:

				X	
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce a single reporting platform at EU level for the compliance with reporting obligations from NIS2:

					X
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce a single reporting platform at EU level for the compliance with reporting obligations from all relevant EU legislation:

					X
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce technical protocols and tools (such as APIs and machine-readable standards) for the purpose of automated reporting by entities to facilitate the integration of reporting obligations into business processes:

				X	
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Align cybersecurity risk-management requirements stemming from relevant EU legislation:

				X	
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce one comprehensive set of rules for cybersecurity risk-management in EU legislation:

			X		
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Introduce a higher level of harmonisation across specific sectors:

			X		
1	*2*	*3*	*4*	*5*	*6*
Least effective					*Most effective*

Please specify which sector (with maximum 20 words):

Financial services.
Regulation should be pragmatic and risk-based, and not just focus on harmonisation.

Q5. Would you suggest any other solutions to remove unnecessary administrative burden further to those mentioned above?

X	Yes	*If yes, please elaborate on your answer (max 100 words):* Reviewing and addressing the duplications and overlaps in reporting requirements between DORA (2022/2554) and the CRA (2024/2847), as well as the clarifying the interplay of DORA (2022/2554) and Solvency II (2009/138) regarding the reporting of third-party risks. The administrative burdens in DORA, especially when filling in the ROI, are not proportionate. Compliance following DORA is too comprehensive and financially burdensome.
	No	
	Do not know/ no opinion	

Insurance Europe is the European insurance and reinsurance federation. Through its 39 member bodies — the national insurance associations — it represents insurance and reinsurance undertakings active in Europe and advocates for policies and conditions that support the sector in delivering value to individuals, businesses, and the broader economy.