FIA response to the European Commission's consultation on the cybersecurity act (CSA) review

Section 2: ECCF

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)?

FIA response: Overlapping cybersecurity regulations in the EU could result in firms having to undertake certification processes for services or products that are covered under existing regulation. The Cyber Resilience Act, for instance, could force financial institutions who provide payment cards in the EU market to undertake a certification due to the trademark rules passing accountability from the payment scheme to the institution. The certification requirements under Article 54(o) and (t) could reflect where there are existing rules within the EU that provide equivalent protections. This is demonstrated via the duplication between the Cyber Resilience Act and Digital Operational Resilience Act where financial services and applications are conflated and produce an unusual application of multiple overlapping rules.

Q6. Do you think European cybersecurity certification should be made mandatory for certain products / services / processes / managed security services?
No

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

From a 1 to 5 scale, FIA proposes to answer 4
Please, elaborate your answer (with maximum 100 words):

FIA response: The ECCF will be affected by the Cyber Resilience Act (CRA) due to the inclusion of financial services within the scope of requiring certifications for designated critical products. This marks the first instance where financial services are encompassed by a product regulation, which will significantly overlap with existing financial regulations, such as the Digital Operational Resilience Act (DORA). DORA is a comprehensive financial regulation that establishes an extensive risk management framework for all financial services and IT infrastructure. The CRA, on the other hand, applies to 'products' or applications and introduces overlapping rules that offer minimal to no cybersecurity benefits to the financial sector. Furthermore, the CRA grants new authority over the financial sector, as market surveillance authorities now have the power to remove financial applications from markets without any intervention from financial regulators.

Section 2.e. Supply chain security

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**
- Risk level has increased significantly
- Don't know / no opinion

Risk of cybersecurity incidents: Although the overall cyber-attack landscape has grown, the risk level has increased slightly. Industry defences, including vendors, have improved over recent years. Improved risk management practices, increased operational resilience investments, and new regulations e.g. DORA has and will continue to translate into the industry managing its supply chain risk more proactively, lowering the residual risk.

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

FIA response: While many software providers run large scale critical services and have robust change control and security practices, some software providers are rushing product releases without comprehensive security built-in or enabled by default. This encourages the following vulnerabilities: inadequately secured authentication tokens vulnerable to theft and reuse; software providers gaining privileged access to customer systems without explicit consent or transparency; and opaque fourth-party vendor dependencies silently expanding this same risk upstream. Providers must urgently reprioritize security, placing it equal to or above launching new products. 'Secure and resilient by design' must go beyond slogans—it requires continuous, demonstrable evidence that controls are working effectively, not simply relying on annual compliance checks.

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

Energy
Transport
Banking
Financial markets infrastructures
Health
Drinking water
Waste water
Digital infrastructure
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
Digital providers

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

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.
Strongly disagree
Disagree
Agree
Strongly Agree
Do not know

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.
Strongly disagree
Disagree
Agree
Strongly Agree
Do not know

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.
Strongly disagree
Disagree
Agree
Strongly Agree
Do not know

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:
(In blue, the Regulation/Directives that most commonly apply to FIA Members.)

Directive (EU) 2022/2555 (Network and Information Security Directive – NIS2)

Regulation (EU) 2022/2554 (Digital Operational Resilience Act – DORA)

Regulation (EU) 2024/2847 (Cyber Resilience Act – CRA)

Directive (EU) 2022/2557 (Critical Entities Resilience Directive – CER)

Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)

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)

Regulation (EU) 2024/1689 (AI Act)

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:**
  FIA response: 3

- **Different incident reporting tools/processes for relevant EU legislation at a national level:**
  FIA response: 2

- **Different incident reporting thresholds defining a reportable/significant/severe incident under the NIS2 Directive and across the different relevant EU legislations:**
  FIA response: 1

- **Implementation of cybersecurity risk-management measures stemming from relevant EU legislation:**
  FIA response: 5

- **Overlap of cybersecurity risk-management measures stemming from relevant EU legislation:**
  FIA response: 4

- **Requirements on how to prove implementation of cybersecurity risk-management measures ('compliance') stemming from relevant EU legislation:**
  FIA response: 6

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

FIA response: DORA and the CRA overlap and apply to the same financial services. The CRA uses product terminology and applies concepts to financial services that are uncertain due to the financial sector being separately regulated and supervised. The CRA further applies another cyber incident reporting regime to financial services despite DORA's objective to harmonise incident reporting in the financial sector. The CRA introduces new enforcement mechanisms and regulators through market surveillance authorities now having a purview over financial services. The CRA creates unclear expectations and would result in a high implementation burden due to substantial guidance being produced during the implementation period.

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?

Yes

No

No opinion

FIA additional response:

- align reporting timelines
- introduce one comprehensive set of rules for incident reporting
- DORA incident reporting has too low thresholds and has resulted in excessive reporting

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

Yes

No

No Opinion

Please, elaborate (with maximum 100 words):

FIA response: Cyber risk management rules should apply from one ruleset if there is overlap and/or the same objectives. DORA and the CRA overlap and apply to the same financial services. The CRA uses product terminology and applies concepts to financial services that are uncertain due to the financial sector being separately regulated and supervised. The CRA further applies another cyber incident reporting regime to financial services despite DORA's objective to harmonise incident reporting in the financial sector. The CRA introduces new enforcement mechanisms and regulators through market surveillance authorities now having a purview over financial services. The CRA creates unclear expectations and would result in a high implementation burden due to substantial guidance being produced during the implementation period. Cyber risk management rules should apply from one ruleset if there is overlap and/or the same objectives.

Q6. Would you agree for the Commission to potentially contact you for further discussion on simplification measures regarding cybersecurity legislation?

Yes

No