Response to IAIS consultation on issues paper on insurance sector operational resilience

Our reference:	EXCO-CS-23-005	Date:	9 January 2023
Related documents:	Public Consultation on Issues Paper on Insurance Sector Operational Resilience		
Contact person:	Kenny Piasecki Policy advisor, General insurance	E-mail:	piasecki@insuranceeurope.eu
Pages:	5	Transparency Register ID no.:	33213703459-54

Consultation questions

1. *General comments on the Issues Paper*

Insurance Europe generally welcomes the IAIS' intention to promote good practices in this area.

One issue of particular importance is the reporting of major ICT-related incidents. In the EU, efforts are being made to ensure that a particular incident must only be reported to a single authority, thereby avoiding undue burden on entities. Supervisory authorities should seek international coordination to the extent possible. However, in the meantime, it is important to give due consideration on how to minimise the burden for the sector. Given the various requests coming from insurance supervisors, a centralisation process at group level should be considered, allowing for a consolidated group answer.

It is also important to avoid imposing new requirements in jurisdictions where the IAIS' objectives have already been met. In that sense, there is a concern that the IAIS approach may result in potential additional data collection requirements, reporting and/or eventually testing and stressing, even though at EU level such requirements are largely, if not fully, covered by the Digital Operational Resilience Act (DORA). This should be avoided.

11. *Comment on Paragraph 7*

It should be acknowledged that insurers generally do not provide critical operations or critical functions comparable to the banking industry. Insurers should be left to determine the business lines or products that are key, given their respective business models and customer impact.

15. *Comment on Paragraph 11*

It should be clarified that critical operations or systems should refer to operations or systems that are essential to the operation of the undertaking, as it would be unable to deliver its services to clients (policyholders, in the case of insurers) without those operations or systems.

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

25. *Comment on Paragraph 19*

An efficient system of governance and organisation is vital for fostering digital operational resilience. However, it should be left to the company to determine the means of achieving this, whether by establishing an independent ICT risk management process within an independent ICT framework, or by supplementing ICT risk management practices in existing structures.

26. *Comment on Paragraph 20*

The principle of proportionality should be part of all supervisors' requests: adopting a proportional and risk-based approach is key when considering any supervisory request. Supervisors' requests must be proportionate to the type, size and financial profile of a relevant legal entity, but also to the digital (including cyber) risks to which it is exposed. Furthermore, the principle of proportionality must also be embedded into the frameworks on cyber incident reporting (paragraphs 61 and 95), penetration testing (paragraph 61), cyber resilience testing (paragraphs 49, 60 and 95) and oversight of IT third-party service providers (paragraph 96).

31 *General comments on Section 3 Key issues and supervisory approaches*

Insurance Europe fully agrees with the need for a greater convergence in cyber governance.

38 *Comment on Paragraph 30*

Digital operational regulation should be principle-based so that it is flexible enough to keep abreast of technological developments and emerging threats.

40 *Comment on Paragraph 32*

There is concern that this point states that training should be part of a supervisory framework, when they should be left in the merit/decision of a company.

42 *Comment on Paragraph 34*

A risk-based approach should be taken to testing, with consideration for the size, business and risk profiles of financial entities.

54 *General comments on Section 3.2.2 Supervisory approaches*

Insurance Europe welcomes this approach, as long as it remains on a voluntary basis.

56 *Comment on Paragraph 43*

Insurance Europe is of the opinion that the suggested approach consisting of publicly disclosing matters of operational resilience is unnecessary.

57 *Comment on Paragraph 44*

Insurance Europe regards as overly prescriptive the requirement to constitute teams responsible for restoration activities.

The seventh bullet point, which refers to reports on training delivered in relation to operational resiliency best practices, should be removed as this information should not be collected by supervisors. In addition, similar concerns arise to those previously mentioned in paragraph 32, where training should be left in the merit/decision of a company.

62 *Comment on Paragraph 48*

Insurance Europe shares the IAIS' view that proportionate requirements are essential because different types of entities are exposed to different types of risks and require different types of protection.

Clarification is needed regarding the forward-looking metrics that are not fully developed: is it the IAIS' intention that these need to be developed and reported upon? To what scope and extent would they need to be developed?

68 *Comment on Paragraph 54*

The insurance industry agrees on the need to aim for a consistent approach to the supervision of cloud service providers, due to their cross-industry importance and high market share.

69 *Comment on Paragraph 55*

As part of existing data calls, the IAIS already collects a wide range of data on cyber on the business side. The entire section alludes to an invitation for another data call for cyber resilience, including potential new metrics. Insurance Europe suggests refraining from imposing new data collection and rather making use of the data already available.

Where regulated firms already share information, insurance supervisors should consider how to share the data that they collect with the insurance industry, so that it can benefit from the available insights: for example, from operational best practices to existing/evolving threats. In the absence of such mechanisms, the purpose of collecting the information is partially defeated as its value is not maximised.

77 *Comment on Paragraph 61*

The first bullet point introduces the possibility of self-assessment questionnaires, which Insurance Europe does not consider to be appropriate tests.

79 *Comment on Paragraph 62*

Insurance firms are unable to monitor and manage the market-wide concentration risk associated with third parties providing services to the financial services industry. Supervisory authorities may, therefore, wish to consider how this issue could be addressed at an international level (potentially building upon the ongoing work in the UK and the EU) to support the cross-border oversight of the services that third parties provide to insurance firms.

There is also support for the development of certification schemes for all ICT third-party providers (TPPs) that could be used as a means of demonstrating compliance with legislation.

93 *Comment on Paragraph 74*

While the IAIS discusses the challenges that supervisory authorities may face in overseeing the services that third parties provide to regulated firms (where such third parties remain outside the regulatory perimeter), the scope of regulated firms' oversight, as per paragraph 75 of the Issues Paper notes, is limited to the matters of their interaction with third parties.

Insurance companies will not have sufficient information on third parties' exposures to other parts of the financial industry and will, therefore, not have a market-wide view of the industry's reliance on third parties. Supervisory authorities may, therefore, wish to consider how this issue could be addressed at an international level (potentially building upon the ongoing work in the UK and the EU) to support the cross-border oversight of the services that third parties provide to insurance firms.

International co-ordination in the development and implementation of operational resilience regulation for third parties will be key to reflect the cross-border nature of such businesses. This should help to introduce substantial efficiencies in the engagement and oversight of third-party arrangements.

Formalising co-operation between jurisdictions will be an essential step towards facilitating international oversight efforts. This could be achieved through creating new or adjusting existing memoranda of understanding between regulatory authorities to capture elements, such as exchange of information, allocation of responsibilities and joint regulatory work in respect of certain types of third parties.

94 *Comment on Paragraph 75*

Insurance Europe invites the IAIS to clarify whether a detailed view of the entire supply chain, including sub-contractors or even fourth or fifth level sub-providers, will be expected from the service recipient, in order to be able to make the systemic concentration risk assessment. From Insurance Europe's perspective, this should not be the case.

112 *Comment on Paragraph 90*

In the third bullet point, the described integration between Business Continuity Management (BCM) functions and business functions is too prescriptive.

In the fourth bullet point, vulnerabilities assessments are mentioned, while in Insurance Europe's opinion there should not be assessments conducted on vulnerabilities.

113 *General Comments on Section 4 Summary of observations and potential future areas of IAIS focus*

Insurance Europe would like to encourage as much consistency as possible between legislation already in place (such as DORA in the EU) and the IAIS recommendations, terminologies and format. This should be done to improve convergence in cyber governance framework, especially regarding reporting requirements.

115 *Comment on Paragraph 92*

Insurance Europe is concerned that the passage "There may be existing IAIS mechanisms for information sharing that could be leveraged for this purpose", may result in an extension of the IAIS data call scope and invites the IAIS to clarify that this is not its intention.

Insurance supervisors should also consider how to share the information that they collect with the insurance industry, so that it can benefit from the available insights: for example, from operational best practices to existing/evolving threats. In the absence of such mechanisms, the purpose of collecting the information is partially defeated as its value is not maximised.

119 *Comment on Paragraph 96*

Insurance Europe supports the IAIS' proposal to consider alignment of reporting definitions and requirements for terms relevant to IT third-party outsourcing. Consistency in concepts and definitions brings efficiencies to the oversight process and ensures that all relevant parties operate within the same set of parameters. This is also an essential ingredient for the development of cross-border co-operation in such an international area as third-party outsourcing.

122 *Consultation Question 1: Do you have views on the relative priority of the observations set out in section 4? Please indicate your preferred prioritisation and any relevant explanations.*

Insurance Europe considers the areas mentioned in Section 4 of as being of equal importance.

a. On information sharing specifically, Insurance Europe asks for harmonisation of reporting requirements coming from regional and/or national supervisors, the FSB and other regulatory bodies.

b. On cyber resilience, Insurance Europe supports using existing supervisory frameworks and information gathered from the group supervisor, rather than an additional regulatory framework and/or standard.

c. On IT third party outsourcing, Insurance Europe fully supports aligning reporting definitions and requirements notably for "critical services", "outsourcing", "third-parties" (paragraph 96), as well as seeking for coherence of supervisory practices and methodologies.

d. On business continuity management, Insurance Europe supports the IAIS' approach.

123 *Consultation question 2: Are there additional observations for potential future IAIS focus that you view as important to address with respect to insurance sector operational resilience, and which have not been identified in this Issues Paper?*

Insurance Europe fully agrees with the need for a greater convergence in cyber resilience framework.

124 *Consultation Question 3: Do you find value in the IAIS facilitating cross-border information sharing to collect information to facilitate a dialogue on operational resilience exposures and best practices? Would you be willing to participate?*

Any IAIS work to facilitate cross-border information sharing is valuable, however this should not duplicate structures that already exist and should be done in a trusted environment where data can be shared and stored in a confidential manner. Moreover, participation should always remain on a voluntary basis.