GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

29 December 2022

GFIA response to IAIS consultation on the Issues Paper on Insurance Sector Operational Resilience

1. General comments on the Issues Paper

GFIA thanks the IAIS for the opportunity to contribute to this consultation. GFIA welcome the IAIS' aim to promote good practices in this area, supports the objectives of this consultation and shares the interests of IAIS in better understanding the issues impacting operational resilience for insurers.

GFIA wishes to emphasise the need to harmonise requirements, the importance of proportionality in regard to supervisory approaches, and a continued understanding of and respect for confidentiality requirements.

One issue of particular importance in the paper is that of reporting of major ICT-related incidents. In the EU, for example, efforts are being made to ensure that a particular incident only needs to be reported to a single authority, thereby avoiding undue burden on entities. While the same approach cannot be mirrored at a global level, it would be important to give due consideration about how to minimise burden for the sector. Regarding requests from insurance supervisors, a centralisation process at group level should be considered, allowing for a consolidated group reply.

It is also important to avoid imposing new requirements in jurisdictions where the objectives the IAIS aims to achieve are already 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, provisions on governance and third-party risk management, even though similar requirements already exist at jurisdictional level. For example, at EU level such requirements are largely if not fully covered by the Digital Operational Resilience Act (DORA). This should be avoided.

3. General comments on Section 1.1 Objectives and Scope

GFIA appreciates the objectives outlined for this consultation and supports the choice of sub-topics related to operational risk. As the Task Force develops this consultation, GFIA notes the importance of proportionality in consideration of supervisory approaches, harmonisation of requirements and respect for confidentiality.

The three areas of focus listed in the paper require specific attention in terms of operational resilience; however given that operational resilience needs to be approached from a critical process perspective, it is important that the implementation is holistic as the lack thereof could result in a suboptimal resilience profile.

In the initial rollout adequate resourcing must be carefully considered as well as the time in which insurers will be expected to comply with any requirements.

Global Federation of Insurance Associations (GFIA)
Secretariat: Rue du Champ de Mars 23, 1050 Brussels, Belgium
Tel: +32 2 894 30 83 E-mail: secretariat@GFIAinsurance.org
www.GFIAinsurance.org

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

8. Comment on Paragraph 4

While cyber-attacks and the challenges associated with them may require heightened focus in the near term, it may also be beneficial for insurers to place sufficient focus on building solid foundations of operational resilience to enable a future fit resilience profile: a key element of which is to empower senior managers to focus on operational resilience.

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.

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.

We suggest to align this definition with existing domestic definitions: for example, such as the EU definition of "critical functions" as "a function the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law".

12. Comment on Paragraph 8

The OSFI's definition of operational resilience "is the ability of a FRFI to deliver its operations, including critical operations, through disruption. It is a prudential outcome of effective operational risk management. For a FRFI to be considered operationally resilient, it must be able to deliver through disruption at least its most critical operations. Operational resilience emphasizes preparation, response, recovery, learning, and adaptation by assuming disruptions, including simultaneous disruptions, will occur. Among other things, it includes resilience to technology and cyber risks."

19. Comment on Paragraph 14

GFIA appreciates the importance of accurate and relevant information and metrics to the work of supervisors. GFIA also echoes the concern voiced here about the increase in ransomware attacks in 2021. GFIA notes that, given the evolving nature of cyber-attacks, the methodology for ascertaining relevant information and metrics must be developed thoughtfully and deliberately, in a manner that is in keeping with the continued development of this nascent operational issue.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

20. Comment on Paragraph 15

A critical part of cyber resilience is a comprehensive understanding of an organisation's IT landscape. This includes the complete mapping of system dependencies, from business processes to servers and databases, together with other infrastructure dependencies. While a business impact assessment process can be leveraged as a starting point, it can cause complications for embedding cyber resilience in organisations where there isn't a proper holistic stock take of IT infrastructure.

21. Comment on Paragraph 16

In addition, as third-party capabilities continue to be entrenched in organisations, there is an integration of value chains, which may require a significant change in the way third parties/outsourcing service providers are viewed, as they are likely to become an extension of the organisation and should, therefore, be managed as such.

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 overall risks profile, the nature, scale and complexity of the services, activities and operations, and the financial profile of a relevant legal entity. The request should also be proportionate to the digital risks, such as cyber risks, it is exposed to. 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).

29. Comment on Paragraph 23

This paragraph states that, in part, "Operational resilience then provides a strategic context for how an entity operates and is a key driver of financial resilience and even of financial stability in some instances."

While effective operational resilience is critical for groups, and the wider insurance sector, this statement appears to take a more expansive view of operational resilience than that used by many regulators and supervisors around the world.

Furthermore, GFIA takes the view that the statement above could be interpreted as suggesting that an operational resilience failure of individual insurance groups would pose financial stability risks. While there are threats to insurers' operational resilience that also pose broader financial stability risks to economies (for example, cyber-attacks), it is doubtful that an operational resilience failure of insurers could pose risks to financial stability.

Therefore, GFIA suggests changing the text above to read "Operational resilience then can provide a strategic context for how an entity operates and is one driver of financial resilience for insurance groups."

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

GFIA emphasises the importance of proportionality and confidentiality when considering various supervisory approaches and frameworks, and notes the need for the harmonisation of requirements to avoid compliance issues and other unintended consequences.

GFIA fully agrees with the need for a greater convergence of the cyber governance framework. However, this convergence must be met in accordance with the initiatives already existing at regional level, notably those in the EU.

33. Comment on Paragraph 26

GFIA appreciates and agrees that these risks are interdependent and interconnected. GFIA supports the idea of an integrated approach to managing operational resilience, and would emphasise the need for proportionality, harmonisation and confidentiality when considering such an approach.

34. Comment on Paragraph 27

Further consideration of how third-party engagement for the provision of critical IT services impacts insurers' cyber resilience is relevant and appropriate. GFIA would, however, emphasise the challenges in recruiting and retaining a limited pool of cyber talent, as is noted later in the consultation. Also, in many cases, third parties can help insurers as many do not have the expertise or resources to develop new technologies.

Any initiative regarding "Managing of ICT third party risk" should consider ongoing initiatives within domestic jurisdictions, for example, DORA at the EU level, and refrain from establishing new requirements.

35. Comment on Paragraph 28

These ideas are worth further thought and consideration, but would need to be further developed and fleshed out, with continued awareness of the role third-parties play in the current cyber landscape for insurers.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

36. Comment on Paragraph 29

GFIA notes that all involved parties need to be aware of the ways these various risks are interdependent and involved in efforts towards risk mitigation.

37. General comments on Section 3.1 Governance and Board accountability

GFIA agrees that robust and effective governance structures play an important role in operational resilience. We note that, in considering the role of such structures, it is important to be mindful of the practical limitations faced by smaller organisations.

While boards and senior management both have important roles in ensuring the implementation of effective operational resilience plans, this section could be improved by additional delineation between the different roles of boards and senior management have relative to each other, the group, and supervisory authorities.

Any proposition should be aligned with existing domestic provisions, for example the provisions of DORA about “ICT risk management”.

38. Comment on Paragraph 30

Digital operational regulation should be principle-based to be 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 it 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.

Any proposition should be aligned with the provisions of ongoing domestic/jurisdictional initiatives.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

43. General Comments on Section 3.1.1 Lessons learnt from the pandemic

Disclosing gaps in the operational resilience profile of an organisation could create other unintended vulnerabilities. These gaps should only be communicated internally with a high-level overview of the operational resilience progress made provided to supervisors.

46. General comments on 3.1.2 Supervisory approaches

GFIA would emphasise the need for confidentiality and proportionality in considering any new or continued supervisory approaches.

47. Comment on Paragraph 37

Apart from oversight, the board and senior management would not manage any other activities related to operational resilience. They do, however, ensure that resources are allocated to those who have a core responsibility to steer the overall operational resilience capability for the organisation.

The BIS Operational Resilience paper requires that financial, technical and other resources are appropriately allocated to support the overall operational resilience approach. This is appropriate and the same applies to insurers.

Third-party expectations/requirements for operational resilience need to be clearly articulated and communicated with relevant third parties and supported by the appropriate third-party governance processes and sufficient rigour to ensure execution and delivery on expectations.

48. General comments on Section 3.2 information collection and sharing among supervisors, public/private collaboration

GFIA notes that consideration of any such collaboration and collection should prioritise respect for confidentiality and proportionality of requirements. The relevant confidentiality requirements must be considered first and foremost when discussing the furtherance of any collaboration or further collection of information. Also, timing for information collection is a concern. In Canada, for example, companies must provide information about an incident within 24 hours. This results in companies focusing on collecting information rather than addressing the incident. Priority should be on the protection of policyholders and containing the incident rather than having discussions with regulators.

Any initiative should aim to encourage best practices and refrain from establishing new requirements, such as additional information channels or multiple layers of reporting.

49. Comment on Paragraph 38

While it makes sense to assist supervisors in consolidating operational resilience information across all insurers to provide stronger oversight, it would equally be important for supervisors to consider the

baseline/as is state of an insurer's operational resilience landscape and posture. There must be some agility applied by supervisors when assessing operational resilience in the context of the insurance environment.

51. Comment on Paragraph 40

GFIA notes that effective information sharing in these areas may help to achieve the results proposed. That said, such information sharing would need to occur in such a way as to not impede on confidentiality for any of the involved parties and that is thoughtful, deliberate, and proportional to the possible effect.

54. General comments on Section 3.2.2 Supervisory approaches

GFIA appreciates that such forums have been effective in certain places and situations. GFIA notes that such an approach would not be the appropriate solution for every forum and that situations must be addressed on a case-by-case basis, and one-size-fits-all supervisory approaches may well not be appropriate for an individual forum. GFIA suggests that the IAIS examine voluntary collaborative approaches that may be equally effective and more appropriately tailored to each forum's situation.

GFIA welcomes this approach, as long as it remains on a voluntary basis, consistent with domestic approaches such as DORA.

56. Comment on Paragraph 43

The suggested approach consisting of publicly disclosing matters of operational resilience is unnecessary. In addition, GFIA notes that, when considering implementing such requirements, supervisors should keep in mind the need for confidentiality and proportionality and avoid unintended consequences for any stakeholders. There is often a voluntary collaborative, cooperative solution that may be possible without additional supervisory requirements.

57. Comment on Paragraph 44

GFIA takes the view that it is overly prescriptive to make teams responsible for restoration activities.

These examples of the types of information to be collected may be more relevant and appropriate to some forums than to others, and GFIA would emphasise the need for any requirements to consider confidentiality and proportionality. Many forums are subject to a regulatory scheme of numerous and sometimes conflicting requirements, and that the harmonisation of requirements (and consideration of existing appropriate supervisory controls) is paramount to promoting optimal compliance.

Also, the suggestion that supervisors collect information on "[r]eports on joint BCP testing/assessment conducted by the insurer and its third-party service providers" might not be feasible since such joint BCP testing/assessments are complicated and rarely conducted.

The seventh bullet point, referring 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.

Currently, BCP testing is conducted separately by insurers and third-party service providers. There are instances from a DR testing perspective where insurers are requested to validate access to systems post failover and failback processes and vice versa. The expectation must be clarified unless the expectation is for insurers to interpret this based on what they deem as feasible and appropriate BCP testing.

See also 31.

58. Comment on Paragraph 45

GFIA notes that laws that limit or prevent the sharing of information beyond an entity or jurisdiction are requirements that must be fully respected as such supervisory approaches are considered. While many of these barriers may impede further supervisory requirements, several of the goals outlined in the consultation may be effectively pursued by a voluntary framework that accounts for the real, practical requirements listed here.

59. General Comments on Section 3.3 Cyber resilience

GFIA agrees that cyber resilience is tremendously important to an organisation's operational resilience framework. GFIA notes that there are inherent challenges in seeking uniformity and consistency in approach in an area that is constantly evolving and still relatively nascent.

Supervisors can gain sufficient assurance through the way in which insurers have:

- Identified their potential cyber risks.
- Ensure that adequate governance processes are in place.
- Comprehensively understand how those risks affect assets.
- Ensure that there are effective mitigating processes in place.
- Create sufficient awareness to cultivate a cyber aware culture.
- Ensure that crisis and incident management processes are in place.
- Regular simulation testing is conducted, gaps identified and actions to address gaps.
- Comply with regulatory requirements related to data protection and confidentiality.
- Ensure that third party service providers comply with the same standard of cyber resilience.

Additionally, skills gaps related to cyber security are a significant challenge in the financial sector in general and perhaps some consideration needs to be given to the steps required to bridge this gap. Perhaps an academy which focuses specifically on developing these skills, sponsored by tech companies who have the experience and the right level of practical tech knowledge in the field.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

61. Comment on Paragraph 47

GFIA would appreciate clarification of the "general consensus" definition. In addition, GFIA would like to confirm that it refers to a consensus of principles and does not refer to a detailed discussion on comprehensive guidelines for implementation and other measures. Although several frameworks and guidelines have been developed and published by various organisations, cyber resilience is not an issue unique to insurers. Therefore, it is desirable for insurance supervisors to maintain consistency and avoid the duplication of guidelines and regulations that have already been developed, or are currently being developed, for (insurer and non-insurer) financial institutions, while allowing for discretionary adjustments according to the specific needs of individual insurers.

62. Comment on Paragraph 48

GFIA supports IAIS's aim to gain assurance in a way that is "proportionate and resource effective." GFIA 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 mentioned 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?

63. Comment on Paragraph 49

GFIA agrees with the idea that "one size fits all" will not work. Duplicative or inconsistent requirements are a real challenge and compliance burden. GFIA agrees that coordination and deliberative, thoughtful study is an appropriate solution.

64. Comment on Paragraph 50

GFIA supports the need for furthered harmonisation and would stress the importance of confidentiality.

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. This approach should be consistent with the regional/jurisdictional initiatives, notably those in the EU.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

69. Comment on Paragraph 55

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

71. Comment on Paragraph 57

GFIA notes that this competition for a limited talent pool is a strain on resources of human capital for all parties.

75. General Comments on Section 3.3.2 Supervisory approaches

GFIA notes that these examples are helpful, but that, of course, every forum will have unique characteristics and needs. GFIA emphasises the need for proportionality and confidentiality in considering supervisory requirements.

76. Comment on Paragraph 60

GFIA supports the continued use of tabletop exercises.

77. Comment on Paragraph 61

GFIA notes that cyber incident reporting requirements are already robust in many forums and that imposing additional reporting requirements may result in unintended consequences or unnecessary compliance burden. GFIA also wishes to stress that laws may prevent such information sharing in this broader manner.

The first bullet point introduces the possibility of self-assessment questionnaires, which GFIA does not consider as falling among appropriate tests.

79. Comment on Paragraph 62

There is the 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.

Any initiative regarding “managing of ICT third party risk” should take into account ongoing initiatives, such as DORA at the EU level, and refrain from establishing new requirements.

Concentration risk of third-party service providers is a reality for most insurers and other institutions which is likely due to the number of available services providers in relation to the services required.

In some instances where insurers leverage existing service providers for other services or additional services, this can likely be because of the existing relationship already in place, scales of economy and to reduce other complexities that could be created through the involvement of other service providers.

81. Comment on Paragraph 64

GFIA notes that these concerns deal with a theoretical future possibility, and emphasise that being thoughtful and deliberative is necessary and further study is needed.

82. Comment on Paragraph 65

Sometimes due to confidentiality of agreements, it is difficult for insurers to know if there is concentration risk.

Furthermore, as contracts are renewed, companies may decide to change providers. Individual companies would not have line of sight into these changes in the entire insurance industry. It would be difficult for companies to be able to track the concentration risk in the industry on an ongoing basis.

90. Comment on Section 3.4.2 Supervisory approaches

GFIA notes the importance of proportionality in any considered supervisory approach, and the fact that any requirements for information sharing must be sensitive to any confidentiality requirements to which insurers may already be subject.

As described in paragraph 67, this is not a problem that can be addressed by the insurance sector alone. Therefore, it is necessary to consider working with other areas of the financial sector to encourage development of third-party service provider regulations, while taking into account the benefits of using such third-party services, and existing or developing regulation, such as that from the EU.

91. Comment on Paragraph 72

This must take into consideration the impact on insurers from an operational perspective.

93. Comment on Paragraph 74

Whilst 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, therefore, will 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 by 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 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.

Regardless of jurisdiction, the risk management processes adopted by third-party service providers must either be above the standard expected by insurers or align with the insurer's expectations.

94. Comment on Paragraph 75

GFIA 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 GFIA's perspective, this should not be the case.

95. Comment on Paragraph 76

Any requirements regarding the provision of specific information must be sensitive to existing legal requirements that may prevent insurers from sharing certain information. Although GFIA appreciates and supports the intention of such requirements, conflicting compliance requirements will only make the current regulatory landscape more problematic.

111. General Comments on Section 3.5.2 Supervisory approaches

GFIA recommends that supervisory approaches generally be cognisant of the fact that every forum is unique and has unique characteristics and approaches, and that any additional supervisory requirements should take into account the existing regulatory regimes that may be in place in a forum as well as any potentially conflicting requirements or laws.

GFIA encourages alignment with ongoing domestic initiatives.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

112. Comment on Paragraph 90

In the third bullet point, the described integration between BCM functions and business functions is too prescriptive.

In the fourth bullet point, vulnerabilities assessments are mentioned, while in GFIA'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

GFIA agrees that alignment of definitions and terminologies may be a useful place to start when considering facilitating information sharing. Such a focus will also allow for productive collaboration without the complication of handling conflicting legal requirements.

GFIA wants to encourage as much consistency as possible with ongoing initiatives at regional level regarding terminologies such as "ICT-related incident", "operational or security payment related incident", "major ICT related incident", "major operational or security payment related incident", "cyber-attack" and "network and information system", as proposed in DORA.

115. Comment on Paragraph 92

GFIA 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 the intention.

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

116. Comment on Paragraph 93

We agree and support the need for harmonisation.

119. Comment on Paragraph 96

GFIA supports the IAIS proposal to consider alignment of reporting definitions and requirements for terms relevant to IT third-party outsourcing (notably with the definitions provided in DORA). 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.

GFIA
GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

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.

GFIA considers that the areas mentioned in Section 4 are of equal importance.

a. On information sharing specifically, GFIA suggests the harmonisation of reporting requirements coming from regional and/or national supervisors, the FSB and other regulatory bodies. Any initiatives should aim to encourage best practices and refrain from establishing new requirements, such as additional information channels or multiple layers of reporting.

b. On cyber resilience, GFIA 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, GFIA fully supports aligning reporting definitions and requirements notably for “critical services”, “outsourcing”, “third-parties” (paragraph 96), as well as seeking for harmonisation of supervisory practices and methodologies (in accordance with European ongoing initiatives for example).

d. On business continuity management, GFIA 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?

GFIA fully agrees with the need for a greater convergence in cyber governance frameworks. However, this convergence must be made in accordance with the initiatives already existing at regional level.

In particular, GFIA would recommend a continued focus on promoting cyber hygiene, including prevention and awareness of insurance policyholders. It is important to recognise that the cyber insurance market is nascent, with high potential growth expectations. Efforts on the prevention side still need to be made so that the impacts of cyber-attacks are mitigated.

We support the fact that the IAIS, in addressing operational resilience issues, takes a clear position against any data nationalism, which weakens industry cyber resilience:

- Reference to the challenges created by related government measures is made in Paragraph 45, but a more in-depth consideration of the issue is warranted.
- Data localisation rules that require data to be stored locally or that certain domestic software be used often impose costs without a commensurate increase in regulatory certainty.
- Furthermore, data nationalism can exacerbate cybersecurity issues, as the onshoring of data can prevent insurers and outsourcing services providers from mitigating the risk through geographic diversification of data storage. In addressing data localisation, the IAIS could consider international agreements on data flows such as those in the US-Mexico-Canada Agreement (USMCA), the APEC Cross-Border Privacy Rules (CBPR) system, or the ASEAN Data Management Framework (DMF), though such systems would need to be tailored specifically for the needs of insurance supervisors and industry.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

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?

GFIA is open to participating in a dialogue on best practices, but notes that information sharing may or may not be appropriate or may need to be limited in accordance with the need for confidentiality and given legal prohibitions on information sharing in certain forums.

Any IAIS work to facilitate cross-border information sharing is valuable, however this should not duplicate structures that are already existing and it 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.

Contacts

Robert Gordon, chair of the GFIA Cyber risks working group (robert.gordon@apci.org)

Marianne Willaert, GFIA secretariat (secretariat@gfiainsurance.org)

About GFIA

The Global Federation of Insurance Associations (GFIA), established in October 2012, represents through its 40 member associations and 1 observer association the interests of insurers and reinsurers in 67 countries. These companies account for around 89% of total insurance premiums worldwide. GFIA is incorporated in Switzerland and its secretariat is based in Brussels.