GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

11 October 2024

GFIA response to IAIS consultation on Draft Operational Resilience Objectives

1 General comments on the Application Paper

GFIA appreciates the opportunity to provide its feedback on the IAIS's draft Application Paper on Operational Resilience. Operational resilience is indeed a critical issue for the insurance industry, and GFIA recognises the importance of the work being undertaken in this area. GFIA understands that this application paper does not establish new supervisory objectives, but rather summarises existing ICP provisions from an operational resilience perspective. As there is no definitive solution to the issue of operational resilience, GFIA asks that the IAIS continues to share the status of its deliberations on this topic with insurers as appropriate. GFIA also asks for continued consistency in the development of the draft Toolkit and the drafting of the AP regarding supervisory practices in late 2024.

As a general comment, the term "critical" is used across the financial industry in multiple contexts. Consistent guidance on how to apply the word "critical" across multiple risk areas would further support operational resilience programmes.

2 General comments on Section 1 Introduction

GFIA is aware that the existing APs contain language such as "APs do not set new standards or expectations, but provide supporting material to assist in the implementation of existing standards". GFIA requests that it be clearly stated in this AP as well.

3 General comments on Section 1.1 Background and purpose

To better support consistency across supervisory authorities, the definition should align with existing regulators' definitions. For example, the Canadian federal regulator OSFI's E-21 Guideline defines operational resilience as the "response of a financial institution and its recovery, by taking a holistic approach that considers all critical operations end to end."

10 Comments on Paragraph 7

As the term "operational resilience" is used extensively in various parts, it should be redefined (or reposted) and clarified in this AP.

11 Comments on Paragraph 8

GFIA expects that a proportional approach will be adopted in the development of supervisory practices in late 2024, taking into account regional and jurisdictional circumstances, rather than adding new requirements, etc.

21 General comments on Section 2.1 Relationship amongst operational resilience, governance, and operational risk management

The communication requirement is too broad, especially regarding regulation authorities.

23 Comments on Paragraph 16

GFIA supports the objective of board oversight regarding an insurer's engagement in operational resilience. This objective is consistent with the US NAIC Insurance Data Security Model Law, which provides that each board must "require its executive management or delegates to develop, implement, and maintain an information security program. The Model Law also provides that each board must require annual reports detailing risk assessment, risk management and control decisions, Third-Party Service Provider

Global Federation of Insurance Associations (GFIA)
Secretariat: rue Montoyer 51, 1000 Brussels, Belgium
Tel: +32 2 894 30 81 E-mail: grant@GFIAinsurance.org
www.GFIAinsurance.org

arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program."

While the emphasis on the role of the board in overseeing operational resilience is appropriate, the paper does not provide sufficient detail on how supervisors will assess the adequacy of board involvement. Insurers need more clarity on the level of reporting and oversight expected, particularly in light of differing governance structures across firms. This section would benefit from more specific guidance on what constitutes effective board engagement in resilience matters, without imposing undue administrative burdens.

26 Comments on Paragraph 18

GFIA supports the objective for insurers to have an approach to operational resilience that is consistent, comprehensive and robust. This is consistent with the US NAIC Insurance Data Security Model Law, which provides that each insurer must "design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control." The Model also specifies a number of security measures insurers must consider, requires that cybersecurity risks be included in the enterprise risk management process, calls for insurers to stay informed on emerging threats and vulnerabilities and for personnel to receive cybersecurity awareness training.

While the integration of operational resilience with the broader risk management framework is mentioned, the paper does not sufficiently address the complexities that insurers face in operationalising this integration. The paper could benefit from more detailed guidance on how these principles will be applied to insurers of varying sizes and structures. It would be useful to clarify the flexibility supervisors will allow in adapting resilience frameworks to different organisational contexts, avoiding a one-size-fits-all approach.

28 Comments on Section 2.2.1

The language found on page 7, "Identifies and documents each critical service end-to-end and the related interdependencies, including, but not limited to, connections with third- and nth-party service providers," seems to imply documenting the subcontracting chain as a whole. GFIA suggests limiting it to "material subcontractors" as in the DORA.

29 Comments on Paragraph 19

In the first bullet, IAIS is using the term "critical service" which is to be used synonymously with Important Business Service (UK – PRA/FCA), Critical or Important Business Service (Ireland – CBI), or Critical Operations (Canada – OSFI). If there was an opportunity for the IAIS to advise regulatory bodies to align on a singular term it would be welcomed.

In the second bullet, the IAIS may want to consider changing 'nth-party' to 'critical nth-party' when mapping critical services. There would be countless 4th, 5th, nth parties to any third-party arrangement. The current wording is ambiguous as it does not distinguish which nth parties should be documented. It is also unclear how organisations will be able to identify interdependencies/connections with nth-party service providers. Due diligence on an organisation's critical services provided by third parties should suffice.

31 Comments on Paragraph 20

GFIA supports the objective for insurers to understand the potential damage that a disruption in critical services can cause. This objective is consistent with the US NAIC Insurance Data Security Model Law, which requires each insurer to "assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information."

In the first bullet, quantifying the maximum disruption/impact for each process may be a challenge for some organisations. Both quantitative and qualitative factors should be considered. Since operational disruption/impact is not always quantifiable, "Quantifies" in the first bullet point should either be revised to

"Understands", or additionally wording should be included to explain that there are cases where it is impossible to quantify maximum disruption/impact.

In the second bullet, regarding "pre-defined", we would like to clarify this means that each entity defines its own "tolerances".

32 Comments on Section 2.2.3

GFIA agrees on the importance of scenario testing with severe but plausible scenarios. On the other hand, it is not easy to prepare exhaustive scenarios because there are many possible factors that can affect operational resilience. Scenario testing is only one of various ways to improve operational resilience, and therefore, instead of preparing exhaustive scenarios, only those scenarios that are truly probable and important should be carefully selected for implementation.

The requirement for insurers to perform self-assessments of their resilience to operational disruptions is reasonable, but the paper lacks specific recommendations on how supervisors will ensure that these assessments are appropriately tailored to the operational realities of each insurer. The guidance should recognise that smaller insurers or those with less complex operations may need different approaches compared to larger, more complex entities. A clearer recognition of proportionality would enhance the practical applicability of the self-assessment framework.

The introduction of the term “severe operational disruption” may lead to confusion. GFIA suggests either maintaining the widely recognised term “severe but plausible” or providing a clear explanation if the new term is intended to have a different meaning. Consistency in terminology is crucial to avoid ambiguity and ensure clear understanding among stakeholders.

33 Comments on Paragraph 21

The IAIS outlines that scenario testing should be embedded to focus on operational resilience and assess the insurer’s ability to withstand and recovery from severe but plausible operational disruptions. This is valid but additional guidance on how this applies specifically to critical services (eg end-to-end testing) would support the role of scenarios in the testing of critical services.

34 Comments on Section 2.2.4

The incident reporting should be limited to major incidents.

35 Comments on Paragraph 22

GFIA supports the objective for insurers to effectively manage cyber incidents, including notifications to regulatory authorities and other stakeholders, even if the incident affects third party service providers. This objective is consistent with the US Insurance Data Security Model Law, which provides that if the incident causes material harm, the NAIC Insurance Data Security Model requires notification to the commissioner and to the consumers. The same applies if the breach happens in a system maintained by a third-party service provider.

Regarding the second bullet, organisations may not be aware of any incident response/reporting with nth parties.

36 Comments on Section 2.2.5

In light of the NIST (National Institute of Standards and Technology) and other general frameworks, it is appropriate to have "identification" before "protection, detection, response, and recovery". Also, with regards to the language, “Reinforces the adoption and maintenance of good cyber hygiene practices (eg identity management, user authentication practices (such as multifactor authentication), access control, attack surface management etc.)”, GFIA suggests referring to “applicable standards” rather than best practices/ examples.

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

37 Comments on Paragraph 23

GFIA supports the objective that requires a robust approach to technology to ensure sensitive and critical information is safely held. This objective is consistent with the US NAIC Insurance Data Security Model Law, which requires each insurer to “Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee’s operations, including: (a) Employee training and management; (b) Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and (c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures.” The Model also requires each insurer to “Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards’ key controls, systems, and procedures.”

Regarding the sixth bullet, this item requires additional clarity. The method for testing the “approach to operational resilience” should be clearly defined.

Paragraph 23 is overly detailed. In addition, various perspectives are described in parallel in bullet points, making it difficult to understand what kind of response will be required. For example, regarding the first bullet point, what is the intention of selecting these categories among many security measures? If internationally used standards are referred to, we suggest clarifying the source and adding a sentence such as "For example, the following approaches could be considered with reference to...".

Generally, measures by people/policies/technologies are considered to be effective. Based on the premise that this paragraph is intended to provide examples, GFIA suggests adding a policy perspective.

38 Comments on Section 2.2.6

The focus on controlled changes is appropriate, but the paper does not sufficiently account for the operational challenges insurers face when implementing these changes. Supervisory expectations regarding the testing and implementation of changes should be more clearly outlined, particularly in terms of what is considered “best practice” without imposing burdensome testing requirements that may disrupt ongoing operations. More flexibility in the application of these guidelines would be welcome, especially for smaller firms.

41 Comments on Paragraph 25

GFIA supports the objective for insurers to have clear recovery and contingency plans in case of a cyber incident. This objective is consistent with the US NAIC Insurance Data Security Model Law, which requires each insurer to establish a written incident response plan designed to recover from any cybersecurity incident.

Regarding the third bullet, it may not be appropriate/feasible for organisations to test the BCPs of its third parties, however it is reasonable to request from the third party the date of the last test and the results.

Regarding "clear recovery objectives", is it correct to understand that insurers are to set RPO（Recovery Point Objective, RTO（Recovery Time Objective), etc., which they consider appropriate?

Finally, insurers are not supposed to validate testing of the BCPs of third parties. In this context, is "confirmation of test results" synonymous with "validation"?

42 Comments on Section 2.2.8

Regarding the language, “Supports effective management of the potential impact of disruption throughout the lifecycle of its relationships with third-party, including intra-group and nth- party, service providers. This lifecycle includes planning, due diligence, and selection, contracting, ongoing monitoring and termination”, this requirement covering the entire contract’s life cycle as well as the whole subcontracting chain seems disproportionate and should be limited to material ICT services supporting critical/major functions.

GFIA suggests replacing "manages" with "oversees" (The second bullet point also mentions "Supports effective management...".).

43 Comments on Paragraph 26

GFIA supports the objective for insurers to manage effective relationships with third-party service providers to maintain the security of information. This objective is consistent with the US NAIC Insurance Data Security Model Law, which provides that “each [insurer] shall exercise due diligence in selecting its Third-Party Service Provider; and an [insurer] shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider.”

Regarding the first bullet, what is the industry-wide definition of “intra-group”? Additionally, the most logical way for organisations to ensure the management and oversight of nth parties is to perform due diligence on their third parties to ensure that the third party is also performing due diligence checks on their third parties. Often, third parties are reluctant to share these details, hence nth parties would be likely to refuse sharing especially since there is no legal relationship between the organisation and the nth party.

The section on third-party risk management highlights an important area, but there is insufficient clarity on the expectations for managing risks from nth-party providers. Many insurers rely on extensive networks of subcontractors, and the current guidance does not adequately address the practical challenges of monitoring and managing these relationships. More explicit guidelines on what is expected from insurers in terms of oversight, without overburdening them with impractical requirements, would strengthen this section.

45 Comments on paragraph 27

What is meant by “macro levels”? Please provide a definition.

47 Comments on Paragraph 28

Please define “supervisor” in this context.

49 Comments on Paragraph 29

GFIA supports the objectives of supervisors, when appropriate, to share information and cooperate with other supervisors to minimise risk. This objective is consistent with the US NAIC Insurance Data Security Model Law, which provides that “the commissioner may share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information.”

GFIA suggests that section 2.3.2 be expanded to focus more on interoperability. Promoting the alignment of operational resilience standards across global regulators should be a key objective, and we encourage the IAIS to use its platform to facilitate greater collaboration among regulators on this issue. This would ensure a more consistent and effective global approach to operational resilience.

While the importance of supervisory cooperation is recognised, there is little detail on how this cooperation will be operationalised in practice, particularly regarding the sharing of real-time operational risk intelligence. Insurers would benefit from clearer guidance on how this information exchange will affect their operations and what is expected from them in terms of data sharing or reporting to supervisory authorities. A more detailed framework for cross-border cooperation would help insurers better navigate regulatory expectations.

51 Comments on Paragraph 30

Regarding paragraph 30 (first bullet point), it is important to enhance the resilience of the entire industry through information sharing. On the other hand, because matters related to operational resilience could also

provide useful hints to cyber attackers, the scope of stakeholders should be carefully limited as necessary when collaborating and transparently communicating with them. Therefore, GFIA proposes to add "taking into account confidentiality" at the end of the sentence.

53 Comments on Paragraph 31

The sentence “Invest in staff training and recruitment to maintain sufficient technical expertise in the areas” should be expanded to include training of staff (including Senior Management) regarding their roles and responsibilities – noted in E-21 s4.1.2 and 4.1.3.

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 42 member associations and 1 observer association the interests of insurers and reinsurers in 68 countries. These companies account for 89% of total insurance premiums worldwide, amounting to more than $4 trillion. GFIA is incorporated in Switzerland and its secretariat is based in Brussels.