December 15, 2022

Dr. Victoria Saporta
Chair, Executive Committee
Mr. Jonathan Dixon
Secretary General
International Association of Insurance Supervisors (IAIS)
c/o Bank for International Settlements
CH-4002 Basel
Switzerland

Dear Dr. Saporta and Mr. Dixon:

The Institute of International Finance (IIF)[1] and its insurance member firms welcome the opportunity to respond to the IAIS's Issues Paper on Insurance Sector Operational Resilience (Issues Paper). Operational resilience is a shared priority of the public and private sectors, as it is essential to maintaining confidence in the insurance sector and the broader financial services industry. Operational resilience is critical to supporting financial stability and sustainable economic growth, benefiting the customers, markets, communities, and broader economies they serve, both nationally and globally.

Key Messages

Operational Resilience as an Outcome. We agree with the IAIS's observations in Paragraphs 11 and 23 of the Issues Paper that operational resilience should be considered, and is increasingly recognized, as an outcome rather than a specific process. An operational resilience approach therefore encompasses the effective management of operational risk, which is focused on reducing risk through preventative measures. These include a wide array of practices and disciplines used by insurers, which enables them to respond, recover, and learn from a negative operational event.

We agree with the suggestion in Paragraph 23 that, building on the principles-based nature of the Insurance Core Principles (ICPs), the IAIS could explore the umbrella concept of operational resilience as an outcome and could discuss and/or set out the links between this outcome-based approach to cyber resilience, IT third-party outsourcing, and business continuity management (BCM). We would welcome further insights by the IAIS on its direction and work plan in this area. The IIF and its members look forward

[1] The Institute of International Finance (IIF) is the global association of the financial industry, with about 400 members from more than 60 countries. The IIF provides its members with innovative research, unparalleled global advocacy, and access to leading industry events that leverage its influential network. Its mission is to support the financial industry in the prudent management of risks; to develop sound industry practices; and to advocate for regulatory, financial, and economic policies that are in the broad interests of its members and foster global financial stability and sustainable economic growth. IIF members include commercial and investment banks, asset managers, insurance companies, professional services firms, exchanges, sovereign wealth funds, hedge funds, central banks, and development banks.

to contributing to the development of a further course of action to promote a holistic approach to operational resilience as an outcome.

Operational resilience is a rapidly changing space, made more complex by the interconnected nature of the risks involved. Insurers should maintain the flexibility to adapt their operational resilience frameworks to the material risks and vulnerabilities that may emerge. We encourage alignment and clear communication between supervisors and insurers as to how a good outcome would be defined. A holistic, outcomes-based approach is also consistent with a dynamic, risk-based, and principles-based framework that allows insurers to properly adapt their operational resilience policies, procedures and processes to emerging risks and vulnerabilities as they evolve.

Operational resilience is first and foremost a natural extension of insurers' risk management expertise. As such, it should remain the responsibility of insurers, supported by risk-focused regulatory guidance and supervisory oversight. Insurers often integrate their operational resilience frameworks into enterprise risk management and governance structures, consistent with the IAIS's focus on an integrated approach to operational resilience in Paragraph 26 of the Issues Paper. However, firms should not be required to adopt any one approach to operational resilience and should be able to determine the specifics of their program and apply that program in a risk-focused manner in a manner that is proportionate to its business model and risk appetite. While strategic decisions, including with respect to the company's risk appetite, usually are made at the Board or Senior Management level, firms should have the flexibility to delegate decision-making to technical teams subject to appropriate reporting and review.

Group-wide approaches to operational resilience allow insurers to leverage global teams and achieve efficiencies in their systems and operations. Group-wide operational resilience programs allow insurance groups to achieve efficiencies from third party service providers, many of which maintain cross-border operations. A group-wide approach to operational resilience benefits insurance supervisors as well, as it offers group supervisors and supervisory colleges a broad and holistic view of the operational resilience framework across the organization. We would encourage the IAIS to recommend to supervisors the removal of any impediment to insurers' use of group-wide solutions for operational or cyber resilience that is not firmly rooted in solvency, sound risk management or policyholder protection considerations.

More generally, we encourage the IAIS to call on its member supervisors to take a dynamic, risk-based, and principles-based approach to the supervision of operational resilience. Overreliance on standardized tools and metrics may overlook emerging threats to sector resilience and may act to constrain insurers' ability to develop new approaches to operational resilience that best suit their unique risk profiles. A principles-based, flexible approach would also accommodate and complement related jurisdictional frameworks, such as the EU's Digital Operational Resilience Act, and other such frameworks that may emerge.

Intragroup and Third-Party Service Providers. We also agree with the IAIS's focus on the importance of intragroup service providers. We would encourage a more flexible approach to the governance of, and internal controls over, those service providers, which generally are governed by group-wide risk management and internal controls protocols, and typically undergo periodic review throughout the lifecycle of the contractual relationship. Intra-group service providers can provide considerable

efficiencies and mitigate the concentration risks of third-party service providers. They can also provide more advanced technologies that would otherwise be beyond the resources of a standalone legal entity.

Critical third parties should be required to demonstrate robust operational risk management and operational resilience approaches to the firms they support. It should be acknowledged that the risks associated with the use of and reliance on third parties and their subcontractors cannot fully be addressed through contractual negotiations. For some critical third-party services, there are a limited set of vendors which may maintain market dominance. Moreover, there can be significant logistical challenges to changing vendors.

When developing expectations for insurers, supervisors should recognize that firms may need to take additional time and actions to gain comfort with some third-party arrangements as a result of some vendors' market dominance. Paragraph 27 and/or Section 3.4 of the Issues Paper could be augmented with the following language:

Supervisors may wish to consider the available mechanisms in their jurisdictions that would improve the ability of insurers to obtain appropriate and needed information from the third parties and their subcontractors in support of insurers' efforts to improve their operational resilience.

One area where regulators and supervisors could provide very helpful input to the industry is with respect to identifying and providing an inventory of potential concentration risks among third-party service providers, given regulators and supervisors' broader view of the sector. An inventory of third-party service providers could also assist with the development of coordinated assurance programs for insurers using the same provider.

Paragraph 77 of the Issues Paper notes that multi-cloud/multi-vendor approaches could mitigate concentration risk, but this discussion should be balanced with an acknowledgement of the considerable costs and operational complexities of adopting those solutions. A requirement for multi-cloud/multi-vendor approaches could undermine the cost effectiveness of using cloud providers or third-party vendors, create less efficient systems, and result in greater vulnerability to cyber threats.

Risks of Geographic Concentration and Data Localization Requirements. As noted in Paragraph 71 of the Issues Paper, geographic concentration can pose significant risk and undue dependence on third-party vendors in a certain jurisdiction. In a similar vein, we would highlight the risks that data localization rules pose to operational resilience. Data localization rules refer to requirements imposed by certain jurisdictions that data be stored on local servers. Such restrictions impose costs on the adoption of innovative technologies that benefit customers and insurers alike and create hurdles to operational resilience. Data localization can lead to complex information technology architectures and system duplication, creating new attack surfaces and sources of risk.

The risks of data localization can be compounded by jurisdictional data security transfer protocols that can be incongruent with, and often lesser than, insurers' own data security standards. Substandard data transfer protocols can compromise customer data and privacy and put corporate security at risk. However, in some jurisdictions, the government or a quasi-governmental entity beyond the insurers'

jurisdictional supervisory authority, may require the transmission of data in an unencrypted form. Other jurisdictions may use older, and often substandard, data transfer methods, such as unsecured Transport Layer Security protocols.

The IAIS should, through discussions with its members and through the Financial Stability Board (FSB), explore available mechanisms for raising awareness of the negative impacts of data localization rules and inadequate jurisdictional data security protocols on the financial sector's operational resilience. The IAIS should also explore with the FSB and other sectoral standard setters the scope for promoting better harmonization of data privacy and security standards and cross-border data flow rules across the financial services sector on a global basis.

Views on Optimal Cross-Sectoral Coordination. We welcome a coordinated approach to operational resilience across the financial services sector, and we commend the cross-sectoral work of the FSB in this regard through its focus on outsourcing and third-party risk management. However, there are some insurance sector specificities that should be reflected in the Issues Paper. Paragraph 7 of the Issues Paper refers to the definition of operational resilience provided by the Basel Committee on Banking Supervision (BCBS), which refers to 'critical operations' and 'critical functions' of a bank. When adapting a definition of operational resilience for the insurance sector, it should be acknowledged that insurers generally do not provide critical operations or critical functions, such as global payments, clearing and settlement infrastructures, the disruption of which could cause severe adverse impacts to the global financial system or the economy. Rather, insurers may have important business lines and insurance products that are necessary to consumers and businesses that they need to protect from disruption. An insurer should determine the business lines or products that are most important, given its business model, strategy and the impact on their customers of a particular business line or product.

The Role of the IAIS. Given the cross-border and cross-sectoral nature of operational resilience, divergences in regulatory standards and supervisory oversight could potentially undermine these efforts. The IAIS can play a critical role in minimizing the risk of regulatory fragmentation in the insurance sector by encouraging the exchange of information among supervisors and developing harmonized approaches to operational resilience.

The Issues Paper highlights the importance of supervisory information sharing in developing effective supervisory strategies for operational resilience oversight. The IIF is particularly familiar with the U.K. Prudential Regulation Authority's and Financial Conduct Authority's Cross Market Operational Resilience Group (CMORG), and we believe it serves a key role in identifying and developing solutions to address operational risks and promoting operational resilience. As noted in Paragraph 45 of the Issues Paper, there is considerable scope to expand supervisory information sharing venues and these venues could assist in the development of a taxonomy, which is noted as an important impediment to effective communication.

In order to facilitate robust and effective information sharing, supervisors should be encouraged to communicate with relevant legislators or regulators when laws or regulations prevent the sharing of information and to suggest amendments that both facilitate appropriate information sharing with trusted parties and protect important national interests. As well, supervisors should consider their ability to liaise

with regulators and supervisors responsible for data protection and privacy requirements in order to discourage the adoption and continuation of data localization rules that can increase operational risk and impede operational resilience and the IAIS should consider available avenues to discuss these issues through the FSB.

Developing Common Definitions and Metrics. We strongly encourage the development of a harmonized lexicon for supervisory discussions of operational resilience, that uses to the extent possible, the definitions provided in the cyber lexicon published by the FSB[2] while recognizing, as noted previously, that certain terminology used in the banking sector is not appropriate for the insurance sector. A harmonized lexicon could facilitate alignment of insurance supervisory frameworks for operational resilience and promote more robust and meaningful dialogue on sectoral trends between the IAIS and other standard setters, and in supervisory colleges.

A common lexicon could also help address the lack of mutual recognition of cyber resilience testing requirements noted in Paragraph 49 of the Issues Paper. Insurers that are subjected to duplicative or inconsistent testing requirements by a number of supervisors must divert resources that could more productively be dedicated to improved cyber resilience. More importantly, as noted in Paragraph 50 of the Issues Paper, inconsistencies in testing requirements could result in cyber vulnerabilities remaining undetected, with consequences that could extend beyond a particular insurer or group of insurers in one jurisdiction.

Any work on common metrics for the insurance sector or any industry data calls in support of the development of common metrics should follow and be based on a common lexicon. Prescriptive metrics should be avoided. However, the use of any metrics by the industry should be voluntary as the same metrics may not be suitable for all insurers, depending on their business models, mix of product offerings, and risk profiles. It should be noted that qualitative information about an insurer's approach to operational resilience can complement a company's or a group's operational resilience framework and often can provide more in-depth insights than purely quantitative data or metrics.

Business Continuity Management. Section 3.5 of the Issues Paper discusses interconnections and interdependencies within systems, participants and service providers operating in the insurance sector, and the need for insurers to adopt sound and prudent management practices to ensure business continuity in the event of an operational incident. As noted above, individual insurers may have limited visibility into these interconnections and interdependencies or into the types of operational incidents that could pose a threat to its important business activities. The industry could benefit from the global view and cross-sectoral oversight maintained by global standard setting bodies, such as the FSB.

When finalizing the Issues Paper, consideration should be given to including a reference to business continuity testing, not only at the firm or group level (as mentioned in Paragraphs 80 and 90), but also at the level of the sector or the broader financial services sector in order to identify interconnections and interdependencies. The IAIS could collaborate with the BCBS and other global standard setting bodies across the financial services sector in order to consider the interdependencies across the global financial

[2] https://www.fsb.org/wp-content/uploads/P121118-1.pdf. We note that the FSB has proposed revisions to the lexicon: https://www.fsb.org/wp-content/uploads/P171022.pdf

system, to develop approaches to business continuity planning that reflect these cross-sectoral dependencies and, more broadly, to discuss the development of common expectations for operational resilience outcomes on a cross-sectoral basis.

Additional Points and Answers to Questions Raised in the Issues Paper

As was emphasized in the IAIS's 2021 GIMAR, insurers responded well to the operational challenges of the pandemic. While the pandemic increased cyber risk and vulnerabilities across sectors, as noted in Sections 1.2 and 3.3.1 of the Issues Paper and in Paragraph 9 of Annex 1, insurers took proactive efforts to address these risks as well as the challenges of the shift to work from home. As with the development of supervisory technology tools (Suptech) during the pandemic to conduct off-site monitoring and data analysis, in a similar fashion, insurers generally pivoted their operations, both internal and customer-facing, in a timely and effective manner. Given the broader successes of these adaptations and innovations, we encourage the IAIS to take a more balanced view of the benefits of digitalization in addition to the risks in Sections 1.2 and 3.3 of the Issues Paper. Digital technologies have contributed to closing insurance protection gaps and promoting financial inclusion, including for small and medium sized businesses, and for individuals and businesses in emerging markets and developing economies.

Paragraph 33 of the Issues Paper calls for a framework for identifying and analyzing the impact of severe but plausible short-, medium-, and long-term risks to operational resilience. We would encourage the IAIS to change the reference to long term risks to horizon scanning in recognition of the difficulty of identifying and addressing uncertain risks that may, if ever, only materialize over a timeframe that far exceeds the business and strategic planning horizon. Horizon scanning is a systematic technique for assessing multiple future scenarios, detecting early signs of potentially important developments (in this case, potentially important operational risks or threats to resilience), and informing appropriate and targeted responses to move towards a more desirable future state.

Our responses to the specific questions raised in the Issues Paper follow.

Do you have views on the relative priority of the observations set out in Section 4?

We encourage the IAIS to prioritize the development of information sharing practices and greater alignment of definitions and terminology related to operational resilience. Ideally, this work would be conducted on a cross-sectoral basis through the FSB. We strongly encourage the development of a harmonized lexicon for supervisory discussions of operational resilience, that uses to the extent possible, the definitions provided in the cyber lexicon published by the FSB[3] while recognizing, as noted above, that certain terminology used in the banking sector is not appropriate for the insurance sector.

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?

[3] Ibid.

The Issues Paper could discuss in more detail the risks to operational resilience posed by data localization rules and substandard data transmission requirements in certain jurisdictions, which may use data security protocols that are incongruent with, and often lesser than, insurers' own data security protocols, as discussed in this response.

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?

The IIF finds considerable value in the IAIS facilitating cross-border information sharing to facilitate a dialogue on operational resilience, and we would be pleased to be part of this dialogue with our insurance members. While there may be a need to restrict membership of some information sharing forums to supervisors, we find considerable merit in public-private forums for information exchange. The IIF participates in the U.S. private sector Financial Services Sector Coordinating Council (FSSCC), which holds joint meetings with the U.S. public sector Financial and Banking Information Infrastructure Committee (FBIIC) to exchange information on threats to homeland security and critical infrastructure, including cyberattacks and risks, and to engage in efforts to improve financial sector resilience and security. (The FBIIC/FSSCC exchanges are broadly similar to the CMORG efforts mentioned above and there is some common membership among the U.S. and U.K. groups.)

The IIF has engaged in a significant amount of work in the areas of operational risk, operational resilience, cyber risk and third-party risk management and we would be pleased to share our work as part of this dialogue and as part of related efforts designed to promote operational resilience in the insurance sector.

The work of a cross-border information sharing group could extend to developing a more aligned taxonomy for operational and cyber resilience, which would greatly benefit both supervisors and the industry. A more aligned taxonomy could facilitate a dialogue on operational resilience exposures and best practices, as the IAIS has suggested.

We welcome the opportunity to comment on this important Issues Paper and would be pleased to discuss our observations in greater detail.

Respectfully submitted,

Mary Frances Monroe