Resolution of Comments for Public Consultation on Insurance Sector Operational Resilience

23 May 2023

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Q1 General comments on the Issues Paper				
1. Insurance Europe	Belgium	No	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, but in the meantime, it is important to give due consideration to 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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
2. Global Federation of Insurance Association	Global	No	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	-Noted and the IAIS thanks respondents for their suggestions for potential future work -See also response to comments 57 and 110 on proportionality and confidentiality

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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. Institute of International Finance	Global	No	Dear Dr. Saporta and Mr. Dixon: The Institute of International Finance (IIF) 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 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	-Noted and the IAIS thanks respondents for their suggestions for potential future work. See also response to comments 57 and 110 on proportionality and confidentiality -Issues Paper terminology reviewed, and updated as necessary, for internal consistency -See also revisions to the Issues Paper at paragraph 78 regarding complexities of multi-cloud / multi-vendor approaches, and section 3.1 regarding Governance and Board Accountability

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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 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	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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 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	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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 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? 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	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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	
4. The Geneva Association	International	No	Thank you for the opportunity to provide feedback on the Issues Paper on Insurance Sector Operational Resilience. An operationally resilient insurance industry is important for maintaining trust in our sector. Insurers, supervisors, and regulators have a mutual interest in making sure the sector is resilient. In this letter we provide our high-level comments as well as answers to some of the questions raised in the consultative document. Management of the Covid crisis by insurers: While there is consensus among insurers, regulators, and supervisors that the insurance industry handled the transition to remote working at the beginning of the pandemic well, and that the insurance industry was ready to respond in this	-The IAIS thanks respondents for their suggestions for potential future work -Regarding comments on the definition of operational resilience, the BCBS text is offered in the Issues Paper as one of several examples for the purpose of general background

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			exceptional situation, without major interruption to clients - the Issues Paper paints an overly negative picture of how insurers managed the switch to remote working. Operational resilience is about acknowledging that there will be disruptions, and to be well prepared for them when these disruptions happen. Whilst the Issues Paper states that "in one-third of the cases, business continuity plans were not prepared for a long-term at-home work force and that one fifth of the financial firms reported that their network operation activities were interrupted during the pandemic", this does not necessarily mean that firms had not planned for extended events. Overall, insurers very quickly adapted to the new way of working and continued to serve their clients while ensuring compliance with local COVID protocols. Definition of Operational resilience: The Issues Paper refers to a definition of operational resilience developed by the Basel Committee on Banking Supervision (BCBS), including "the ability of a bank to deliver critical operations through disruption" and "in considering its operational resilience, a bank should assume that disruptions will occur, and take into account its overall risk appetite and tolerance for disruption". While we acknowledge that the BCBS (and other definitions) are provided for illustrative purposes - we think it is important to highlight that bank operations (including payment infrastructure) are very different from insurance operations (not a critical function). Existing operational resilience requirements: EU-based insurance companies deal already with operational resilience requirements as part of Solvency II (i.e., ORSA process) as well as with DORA (EU Digital Operational Resilience Act) entering into force soon. Another example is the UK operational resilience regime, which entered into force in March 2022 and requires financial institutions within its scope, including insurers, to identify important business services; set impact tolerances for disruption; and identify vulnerabilities in their operational resilience. References to these existing requirements are, however, not made within the IAIS Issues Paper. There are several jurisdictional approaches to ensuring and enhancing operational resilience in the re/insurance industry. As a globally interconnected industry it is key for us that any potential regulatory and supervisory fragmentation can be avoided and hence harmonization, while ensuring flexibility to consider company-specific characteristics, is key. IT third-party outsourcing: Since the beginning of the pandemic, we have seen an increase in the number of cyber-attacks carried out - among others due to an increased attack-surface resulting	-Regarding comments on existing operational resilience requirements, the Issues Paper acknowledges the EU's Digital Operational Resilience Act (DORA) at Paragraph 61 and 77 -Regarding comments on IT third-party outsourcing, the Issues Paper acknowledges that both legacy systems and outsourcing may present challenges and opportunities with regards to operational resilience at paragraphs 28 60 and 71 -Regarding comments on the principle of proportionality, see responses to comments 57 and 110

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			from digitalization of businesses. The Issues Paper focuses on IT outsourcing, including to so-called critical third parties and concentration risks. Outsourcing to third party IT providers seems to get an exceptional amount of scrutiny. While the outage of a cloud provider might present a risk, legacy on premise systems that are not designed in a geo-redundant manner could be equally risky, if not riskier, depending on the circumstances. Importantly, concentration risks are not limited to IT providers but may also exist in other areas. In addition, the Issues Paper would benefit from convergence in some key definitions, notably for the term "critical" which is used for "critical IT services" (para 16, 27, 29 and 62) and "critical third-parties" (para 28, 35 and 96). Equally, the term "threat" which is used for "potential threats" (para 38), "cyber threats" (para 40), "systemic threats", "threat led penetration tests" (para 61) and "threat actors" (paragraph 95) would benefit from a clear definition. Data transfer to government agencies Global insurers are subject to varying local jurisdictional data and reporting requirements, including for sensitive data to be transmitted to certain regulatory authorities or government agencies. The data ranges from regulatory reporting to customer information that is then made available to the customer through government run portals. In several cases the data is transferred in a manner that does not meet insurers' own data security requirements. Such data transfers put consumer data as well as insurers' corporate security at risk, besides creating a barrier in doing business in certain jurisdictions. Examples include data transmissions using outdated and unsecured protocols, unencrypted transfers, or weak security of web portals used by government agencies. Principle of proportionality: We welcome the IAIS' efforts to increase the harmonization of supervisory practices. As stated in 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. Supervisory frameworks need to consider the rapidly changing threat landscapes focusing on core principles and avoiding too specific or prescriptive technical requirements. A one-size-fits-all approach would not be successful. Supervisors' requests must be proportionate to the type, size, and financial profile of a relevant legal entity, and the digital (including cyber) risks it is exposed to. While not explicitly stated, certain sections within the paper hint at potential additional data collection exercises to create metrics, notably paragraphs	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			48, 55 and 95. We would caution against increased data collection exercises, particularly if the additional burden place in the industry is not proportionate to the risk it tries to capture. Responses to select targeted questions: Question: 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? Answer: Whilst the IAIS discusses the challenges that supervisory authorities may face in overseeing the services that third parties provide to the regulated firms (where such third parties remain outside the regulatory perimeter), the scope of regulated firms' oversight, as 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 the international level (potentially building on 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 and reduce the gaps in oversight which could result from a less uncoordinated approach. -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.	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			Question: 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? -Answer: Information exchange is essential for the effective oversight of firms' operational resilience which is often tied with the third parties that operate internationally. In this context, 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, 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. We thank the IAIS for the opportunity to provide feedback and look forward to further engagement on this and other topics.	
5. General Insurance Association of Japan	Japan	No	We appreciate the development of the IP and the opportunity to give feedback on it. We think the description is generally acceptable. However, when implementing new measures and structures, insurance sector-specific issues, the situation of each individual insurer including resources, and feasibility should be taken into consideration. In addition, as discussions regarding a core solution to the operational resilience issue are ongoing, we would like the IAIS to share the discussion details with insurers, as appropriate.	-Noted
7. DGSFP	Spain	No	We agree on the messages given in the Paper.	-Noted
8. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	The paper introduces new terms that may not be familiar to some readers. Suggest adding a glossary to the beginning of the paper. "Business Continuity Management" (BCM) is a concept mentioned throughout the paper and in some places, "Business Continuity Planning" (BCP) is used as an interchangeable term. Suggest defining these two terms in a glossary and also clarifying in the paper (see comments for paragraphs 35 and 80) the difference between the two. Presumably BCM encompasses BCP. There are numerous inconsistencies in the use of the Oxford comma (a.k.a. serial	-See revisions at paragraph 17 of the Issues Paper -Issues Paper reviewed for consistency with respect to the use of the Oxford and Serial comma.

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			comma) throughout the document. For example, paragraphs 25 and 29 omit it, while paragraphs 2 and 24 employ it.	
Q2 General comments on Section 1 Introduction				
Q3 General comments on Section 1.1 Objectives and Scope				
10. Global Federation of Insurance Association	Global	No	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.	-In response to the comment that "[i]n 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," it is noted that IAIS guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory material -See also the responses to comments 57 and 110 on proportionality and confidentiality
11. Institute of International Finance	Global	No	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	-Noted and see also revisions at paragraph 5 and section 3.1 of the Issues Paper, which address the roles of the Board and Senior Management

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			insights by the IAIS on its direction and work plan in this area. The IIF and its members look forward 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.	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
Q4 Comment on Paragraph 1				
14. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	In the second bullet, add "IT" before "Third-party outsourcing" as this is way the topic is framed throughout the paper and especially in the heading for Section 3.4	-Agreed
Q5 Comment on Paragraph 2				
Q6 Comment on Paragraph 3				
17. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest the following edit to this paragraph. Based on the preceding text, the area of expertise of the stakeholders is implied. Delete "operational resilience." "The information in this paper is informed by a review of the IAIS Insurance Core Principles (ICPs), a stocktake of existing publications by Standard Setting Bodies (SSBs) with relevance to operational resilience, direct engagement - including roundtables - held with experts external to the IAIS membership, and information shared on supervisory practices among insurance supervisors."	-Agreed
Q7 General comments on Section 1.2 Relevance of operational resilience to the insurance sector				
Q8 Comment on Paragraph 4				
19. Global Federation of Insurance Association	Global	No	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	-See revisions at paragraph 5 and 6 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			profile: a key element of which is to empower senior managers to focus on operational resilience.	
21. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest the following edit to the second sentence to improve flow: "The concept of operational resilience is not new, though recognition of the importance of adapting supervisory regimes to account for the growing reliance by insurers on digital systems is more recent."	-Agreed
Q9 Comment on Paragraph 5				
22. General Insurance Association of Japan	Japan	No	Given the context, we believe that "Cyber attacks grew with the spread of the pandemic" should be revised to "Cyber attacks grew with the spread of the pandemic and the accompanying widespread adoption of remote working".	-Agreed
24. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	It might strengthen this paragraph to have similar statistics on cyber-attacks between 2019 and 2020, if available, to give some pre-pandemic context. Also, this paragraph is a bit disjointed; there is a number in February and a number in late April, but then goes to the percent increase in May and June compared to March and April. Since the number for March isn't given anywhere, it is hard to know what kind of increase it is over March. For consistency with the use of percent signs elsewhere within the document, suggest replacing "per cent" with a percent sign. Replace "cyber attacks" with "cyber-attacks" for consistency with the other eight occurrences of this word throughout the document.	-Agreed
Q10 Comment on Paragraph 6				
Q11 Comment on Paragraph 7				
26. Insurance Europe	Belgium	No	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.	-The BCBS definition is included as an example only and the Issues Paper does not attempt to define critical operations

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
				-See also revisions at paragraphs 63-65 of the Issues Pape
27. Global Federation of Insurance Association	Global	No	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".	-The Issues Paper does not attempt to define critical operations -See also revisions at paragraphs 63-65 of the Issues Pape
Q12 Comment on Paragraph 8				
29. Global Federation of Insurance Association	Global	No	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."	-Noted
Q13 Comment on Paragraph 9				
Q14 Comment on Paragraph 10				
Q15 Comment on Paragraph 11				

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
33. Insurance Europe	Belgium	No	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.	-The Issues Paper does not attempt to define critical operations -See also revisions at paragraphs 63-65 of the Issues Pape
Q16 General comments on Section 1.3 Issues Paper structure				
Q17 Comment on Paragraph 12				
Q18 Comment on Paragraph 13				
Q19 Comment on Paragraph 14				
39. Global Federation of Insurance Association	Global	No	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.	-Noted
41. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Replace both occurrences of "cyber attacks" with "cyber-attacks" for consistency with the other eight occurrences of this word throughout the document.	-Agreed
Q20 Comment on Paragraph 15				
42. Global Federation of Insurance Association	Global	No	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.	-The IAIS Application Paper on Supervision of Insurer Cybersecurity (2018), referenced in the Issues Paper, states at paragraph 103 that “[t]o the extent practicable, the insurer should identify and maintain a current inventory or mapping of its information assets and system

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
				configurations, including interconnections with other internal and external systems, in order to know at all times the assets that support its business functions and processes. The insurer should carry out a risk assessment of those assets and classify them in terms of criticality."
44. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest the following edit (deleting "to insurers") to the first sentence to improve flow: "The risks posed by a third-party outsourcing partner for IT-related functions are similar across many industries, including the insurance industry." In this paragraph, consider adding a bit more context around "concentration risk" as the concept is being introduced here.	-Agreed
Q21 Comment on Paragraph 16				
45. Global Federation of Insurance Association	Global	No	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.	-Noted
47. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest the following edit to the last sentence; removing "business continuity" eliminates a redundancy and also broadens this statement a bit. "However, a critical piece of moving to hybrid and remote work environments is understanding and proactively managing the risks that arise from an increased attack surface and reliance on technology and outsourcing of critical IT services."	-Agreed
Q22 Comment on Paragraph 17				
Q23 General comments on Section 2 Applicability of ICPs to operational resilience				
Q24 Comment on Paragraph 18				

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Q25 Comment on Paragraph 19				
51. Insurance Europe	Belgium	No	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.	-Noted
52. Global Federation of Insurance Association	Global	No	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.	-Noted
Q26 Comment on Paragraph 20				
54. Insurance Europe	Belgium	No	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).	-See response to comments 57 and 110
55. Global Federation of Insurance Association	Global	No	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).	-See response to comments 57 110
57. National Association of Insurance	USA, NAIC	No	Suggest the following edit to the second sentence; modifier not needed.	-Agreed

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Commissioners (NAIC)			"All of which promote operational risk management more generally, while respecting issues of proportionality."	
Q27 Comment on Paragraph 21				
59. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	The ICPs typically use "sound" in referring to an insurer's management, governance, etc., but not when describing supervision. "The ICPs identified as supporting the supervision and sound management of operational resilience in the insurance sector include:"	-Agreed
Q28 Comment on Paragraph 22				
61. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Similar to paragraph 20, the modifier "sound" is not really needed here. "The ICPs have clear interactions with operational resilience and support the management of an insurer's operational risks."	-Agreed
Q29 Comment on Paragraph 23				
62. Global Federation of Insurance Association	Global	No	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	-See revisions at paragraph 24 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			then can provide a strategic context for how an entity operates and is one driver of financial resilience for insurance groups."	
Q30 Comment on Paragraph 24				
65. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Similar to paragraph 21, delete the modifier "sound" in this context. "The review of ICPs also revealed a number of examples of areas where further discussions or considerations for developing supporting materials could advance the supervision of cyber resilience, IT third-party outsourcing, and BCM as critical elements of operational risk management (which are considered among those elements outlined in section 4)."	-Agreed
Q31 General comments on Section 3 Key issues and supervisory approaches				
66. Insurance Europe	Belgium	No	Insurance Europe fully agrees with the need for a greater convergence in cyber governance.	-Noted
67. Global Federation of Insurance Association	Global	No	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.	-See responses to comments 57 and 110 on proportionality and confidentiality
68. Institute of International Finance	Global	No	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	-See response at comment 3

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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	

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
Q32 Comment on Paragraph 25				
Q33 Comment on Paragraph 26				
71. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work -See also response to comments 57 and 110
Q34 Comment on Paragraph 27				
73. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
74. Institute of International Finance	Global	No	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.	-See response to comment 3
76. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest the following edit to the last sentence to improve clarity (addition of the word "customer"): "This is particularly important for insurers, in respect of any confidential or personal customer data that is shared with third-party service providers." Inclusion of the word "legacy" in the second sentence implies that all on-premises IT infrastructure is ipso facto obsolete, unable to be updated, nonconforming to security standards, inherently vulnerable, unsupported, unscalable, etc. This simply should not be presumed. The use of advancing technologies could provide cyber security benefit as compared to in-house technology infrastructure and systems, whether legacy or not. "The use of advancing technologies, such as the cloud, could provide efficiencies and improvements in cyber security as compared to on-premises technology infrastructure and systems."	-See revisions at paragraph 28 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Q35 Comment on Paragraph 28				
77. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q36 Comment on Paragraph 29				
79. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
81. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	See general comments above and for paragraph 80 - BCP is introduced here without explaining its relationship to BCM. It is also used somewhat interchangeably with BCM. Recommend adding a sentence clarifying the difference between BCM and BCP in this paragraph.	-See revisions at paragraph 17 of the issues Paper -See also response to comment 8
Q37 General comments on Section 3.1 Governance and Board accountability				
82. Global Federation of Insurance Association	Global	No	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".	-Revised paragraph 5 and revised section 3.1 of the Issues Paper address the roles of the Board and Senior Management -See also revisions at paragraph 32 of the Issues Paper
Q38 Comment on Paragraph 30				
84. Insurance Europe	Belgium	No	Digital operational regulation should be principle-based so that it is flexible enough to keep abreast of technological developments and emerging threats.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
85. Global Federation of Insurance Association	Global	No	Digital operational regulation should be principle-based to be flexible enough to keep abreast of technological developments and emerging threats.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q39 Comment on Paragraph 31				
Q40 Comment on Paragraph 32				
88. Insurance Europe	Belgium	No	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.	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and not meant to create expectations on how supervisors should implement supervisory material
89. Global Federation of Insurance Association	Global	No	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.	-See response to comment 88
91. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	The document mentions sound operational resilience, sound practices, sound operational risk management, sound governance, sound management, sound supervision etc., but the word appears misplaced in the following sentence. It should be moved as follows. "Recognising that operational disruptions can have widespread impacts across an organisation, the provision of appropriate training across relevant groups within an organisation could facilitate the implementation of a sound operational resilience framework."	-See revisions at paragraph 33 of the Issues Paper
Q41 Comment on Paragraph 33				

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
92. Institute of International Finance	Global	No	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.	-See revisions at paragraph 34 of the Issues Paper
94. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest the following edit to the first sentence to eliminate redundancy: "The absence of a framework for identifying - and analysing the impact of - severe but plausible short, medium and long-term risks can limit the chances of successfully enhancing the insurer's overall operational resilience."	-See revisions at paragraph 34 of the Issues Paper
Q42 Comment on Paragraph 34				
95. Insurance Europe	Belgium	No	A risk-based approach should be taken to testing, with consideration for the size, business and risk profiles of financial entities.	-See revisions at paragraph 35 of the Issues Paper
96. Global Federation of Insurance Association	Global	No	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.	-See revisions at paragraph 35 of the Issues Paper
97. General Insurance Association of Japan	Japan	No	Regarding stress testing scenarios, as risks can vary significantly according to jurisdiction and insurer, detailed scenarios should be tailored to individual circumstances. As such, we propose that the second sentence be revised as follows: Detailed scenarios for testing should be developed to suit each individual insurer´s situation, given that risks vary widely according to jurisdiction and insurer. It should also be accompanied by appropriate follow-up investment to remedy identified gaps.	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and not meant to create expectations on how supervisors should implement supervisory material
Q43 General Comments on Section 3.1.1 Lessons learnt from the pandemic				

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
99. Global Federation of Insurance Association	Global	No	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.	-Noted
100. Institute of International Finance	Global	No	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.	-Noted
Q44 Comment on Paragraph 35				
Q45 Comment on Paragraph 36				
Q46 General comments on 3.1.2 Supervisory approaches				
104. Global Federation of Insurance Association	Global	No	GFIA would emphasise the need for confidentiality and proportionality in considering any new or continued supervisory approaches.	-See response to comments 57 and 110
Q47 Comment on Paragraph 37				
106. Global Federation of Insurance Association	Global	No	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	-See revisions at paragraph 38 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
107. General Insurance Association of Japan	Japan	No	In Paragraph 32, it is stated that "While each individual member of the Board or Senior Management should not reasonably be expected to have expertise in operational risk management, Boards collectively should possess adequate knowledge, skills, and experience to provide constructive oversight to Senior Management who make decisions that have consequences on an insurer's operational resilience." Therefore, "senior management" in the first bullet point should be deleted.	-Expectations that the Board and Senior Management have the appropriate knowledge and skills, as set out at Paragraph 33 of the Issues Paper is consistent with existing ICP 7
109. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Replace "oversight over" with "oversight of" in the first sentence to eliminate the nearly redundant alliteration: "Many supervisory authorities currently seek assurance that insurers have sound governance frameworks and adequate Board and Senior Management oversight of resilience measures, as well as strategies to mitigate risks associated with operational disruption." Additionally, just having and documenting processes isn't enough, so recommend adding a bullet regarding the importance of regularly reviewing/updating processes.	-See revisions at paragraph 38 of the Issues Paper
Q48 General Comments on Section 3.2 Information collection and sharing among supervisors, public/private collaboration				
110. Global Federation of Insurance Association	Global	No	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.	-Existing ICPs underscore the concepts of proportionality and confidentiality (see ICPs overarching concepts paragraphs 9-10 and ICP 3) -See also response to comment 57

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			Any initiative should aim to encourage best practices and refrain from establishing new requirements, such as additional information channels or multiple layers of reporting.	
111. Institute of International Finance	Global	No	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.	-The BCBS definition is included as an example only and the Issues Paper does not attempt to define critical operations -The IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
113. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Recommend shortening this section name for clarity and consistency with other section titles: "3.2 Information collection and sharing"	-Agreed
Q49 Comment on Paragraph 38				
114. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
115. General Insurance Association of Japan	Japan	No	Access to various types of information, including potential threats, should be well coordinated in advance, taking into account the system impact and potential burden on the insurer.	-Noted
Q50 Comment on Paragraph 39				
119. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Regarding supervisor and insurer engagement, it seems that in most cases the appropriate engagement is between the supervisor and insurer management (not the board), though the board of course should have a clear understanding of the insurer's operational resilience framework (this is mentioned elsewhere in the paper). "To gather this information, some supervisors proactively engage with an entity's	-Noted -See also revised text at Section 3.1 of the Issues Paper which addresses the roles of the Board and Senior Management

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			Senior Management to understand the effectiveness of an entity's operational resilience framework."	
Q51 Comment on Paragraph 40				
120. Global Federation of Insurance Association	Global	No	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.	-Noted and with regards to proportionality and confidentiality see also responses to comments 57 and 110
121. General Insurance Association of Japan	Japan	No	It is important to enhance industry-wide resilience through information sharing. At the same time, however, information sharing should be limited to what is truly necessary to avoid an excessive burden on insurers. In addition, the necessity of information sharing among supervisors should be fully considered, and information should be shared carefully with appropriate safeguards applied.	-Noted and with regards to proportionality and confidentiality see also responses to comments 57 and 110
123. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Last sentence, beginning and end quotes should be consistent: As the International Monetary Fund (IMF) has noted "[a]ttackers show a degree of agility in cooperation across borders that authorities find difficult to match.'"11	-Agreed
Q52 General comment on Section 3.2.1 Lessons learnt from the pandemic				
Q53 Comment on Paragraph 41				
Q54 General comments on Section 3.2.2 Supervisory approaches				
126. Insurance Europe	Belgium	No	Insurance Europe welcomes this approach, as long as it remains on a voluntary basis.	-Noted
127. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Q55 Comment on Paragraph 42				
129. General Insurance Association of Japan	Japan	No	When holding the forum, consideration should be given to the operational conditions of each insurer in terms of implementation procedures (e.g., frequency, participant selection, ensuring anonymity in information sharing, and defining cases that should be shared) so as not to impose an excessive workload on insurers.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q56 Comment on Paragraph 43				
131. Insurance Europe	Belgium	No	Insurance Europe is of the opinion that the suggested approach consisting of publicly disclosing matters of operational resilience is unnecessary.	-Noted
132. Global Federation of Insurance Association	Global	No	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.	-Noted and see responses to comments 57 and 110 on proportionality and confidentiality
133. General Insurance Association of Japan	Japan	No	Regardless of the discloser (e.g., insurer or regulator) or the content (e.g., weaknesses or response status), it is not desirable to widely publicize matters that could affect operational resilience, as this could lead cyber attackers obtaining clues. Therefore, if supervisory authorities publicize reports from an insurer, they should carefully consider the above effects and apply appropriate safeguards. When supervisory authorities request reports from insurers, consideration should be given to limit the scope of such reports to what is truly necessary so as not to impose an excessive burden on insurers.	-Noted and see responses to comments 57 and 110 on proportionality and confidentiality
Q57 Comment on Paragraph 44				
135. Insurance Europe	Belgium	No	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.	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory material.

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
136. Global Federation of Insurance Association	Global	No	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.	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory material.
137. General Insurance Association of Japan	Japan	No	When supervisory authorities request information disclosure from insurers, we request that they clarify the purpose, and ensure that the scope is reasonable so as not to impose an excessive burden on insurers. Therefore, we propose that the first sentence be revised as follows: With respect to supervisory frameworks on operational resilience, supervisors may collect a range of information, to the extent necessary but within reason, including:	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory material.
139. National Association of	USA, NAIC	No	The seventh bullet point references operational resiliency, rather than operational resilience, which appears 79 times throughout the document. Therefore, replace	-Agreed

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Insurance Commissioners (NAIC)			"resiliency" with "resilience" for consistency. "Reports on training delivered in relation to operational resilience best practices, and in particular on expectations, and roles and responsibilities during periods of sub-optimal functioning;"	
Q58 Comment on Paragraph 45				
140. Global Federation of Insurance Association	Global	No	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.	-Noted
143. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Consider adding "consumer" to the second bullet point as follows: "Concerns on data protection and consumer privacy laws that limit or prevent the sharing of information beyond an entity or jurisdiction" Further, consider adding an additional bullet as an additional barrier: - Hesitancy of insurer to share information with supervisor because of concerns the information could lead to additional scrutiny of their controls, or that doing so could cause legal risks;	-See revisions at paragraph 46 of the Issues Paper
Q59 General Comments on Section 3.3 Cyber resilience				
144. Global Federation of Insurance Association	Global	No	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.	Noted

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			? 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.	
Q60 Comment on Paragraph 46				
147. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	We may be further away from the pandemic once this paper is published, so recommend deleting "has" in the first sentence. Also in the first sentence, there should be a comma after "technologies" to separate the two independent clauses. "The insurance sector is heavily dependent on the use of digital technologies, and this reliance only accelerated during the pandemic as entities transitioned to remote working."	-Agreed
Q61 Comment on Paragraph 47				
148. Global Federation of Insurance Association	Global	No	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.	-See revisions at paragraph 48 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
149. General Insurance Association of Japan	Japan	No	We would appreciate clarification of the "general consensus" definition. In addition, we 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 organizations, 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 for (non-insurer) financial institutions, while allowing for discretionary adjustments according to the specific needs of individual insurers.	-See response to comment 148
Q62 Comment on Paragraph 48				
151. Insurance Europe	Belgium	No	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?	-Noted and the IAIS thanks respondents for their suggestions for potential future work
152. Global Federation of Insurance Association	Global	No	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?	-Noted and the IAIS thanks respondents for their suggestions for potential future work
153. General Insurance Association of Japan	Japan	No	It is stated that "widely agreed, standardised, forward-looking metrics are not fully developed", but we believe that it is quite difficult to evaluate a rapidly changing cyber-attack with "metrics". Even if effort is devoted to the development of metrics, they are unlikely to be effective.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q63 Comment on Paragraph 49				
155. Global Federation of	Global	No	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.	-Noted

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Insurance Association				
156. General Insurance Association of Japan	Japan	No	As it would be beneficial, we hope that supervisory coordination (especially mutual recognition of cyber resilience testing requirements) will be discussed in the future. At the same time, it is necessary to ensure that the framework does not place an excessive burden on insurers.	-Noted
Q64 Comment on Paragraph 50				
158. Global Federation of Insurance Association	Global	No	GFIA supports the need for furthered harmonisation and would stress the importance of confidentiality.	-Noted
Q65 Comment on Paragraph 51				
Q66 Comment on Paragraph 52				
Q67 Comment on Paragraph 53				
162. General Insurance Association of Japan	Japan	No	Since the characteristics of systems maintained within the insurance industry vary widely and it is desirable to take measures according to risks, it is recommended that insurers have discretion in planning the frequency and content of testing, taking into account not only cyber resilience but also the impact of cyber incidents on the insurer and the jurisdiction where the cyber incident occurs. In addition, we would like to confirm that the future direction of monitoring does not envision an approach that requires insurers to report in detail.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q68 Comment on Paragraph 54				
164. Insurance Europe	Belgium	No	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.	-Noted
165. Global Federation of Insurance Association	Global	No	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.	-Noted

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
166. Institute of International Finance	Global	No	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 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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work and see revisions at paragraph 56 of the Issues Paper
167. General Insurance Association of Japan	Japan	No	If third-party service providers are to be used, consideration should be given to the fact that the implementation of "on-site inspections" may not be acceptable in some cases due to the contract between third-party service providers and insurers, or the various regulations of the third-party service. We would like to confirm that the "supervisory cyber assurance methods" listed here are examples only.	-See revisions at paragraph 55 of the Issues Paper
169. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	For this paragraph and heading, it might be more appropriate to refer to "consistent approach" rather than "standardized metrics" to be less prescriptive. The use of "consistent approach" is also more outcomes focused. "Lack of consistent approach	-See revised heading above paragraph 53 and deleted heading above paragraph 55 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			Having a consistent approach to assess insurers' cyber resilience can be helpful especially when insurers are engaging third-party service providers that operate cross jurisdiction (eg cloud)."	
Q69 Comment on Paragraph 55				
170. Insurance Europe	Belgium	No	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.	-Noted
171. Global Federation of Insurance Association	Global	No	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.	-Noted
172. General Insurance Association of Japan	Japan	No	We agree that quantitative metrics are helpful in assessing parts of an insurer's cyber resilience framework, and in understanding inherent and residual risk, maturity of risk management frameworks, and identification of potential concentration risk. On the other hand, even if more metrics including forward-looking ones are developed and defined in other sectors, it is quite possible that they may not be appropriate for quantitative metrics due to insurance-specific characteristics. Therefore, quantitative metrics developed in other sectors should be thoroughly scrutinized by the insurance industry. As for availability, which is generally given as an available indicator, we do not have a specific image of the calculation process, given the nature of cyber-attacks, where the probability of occurrence is difficult to predict.	-Noted
174. National Association of	USA, NAIC	No	Punctuation is inconsistent. An en dash follows Availability in the first bullet point, while a simple hyphen follows RTO and RPO in the second and third bullet points. All	-Agreed

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Insurance Commissioners (NAIC)			should be en dash characters to maintain consistency with the remainder of the document. Recovery Time Objective (RTO) - defined by the entity… Recovery Point Objective (RPO) - defined by the entity…	
Q70 Comment on Paragraph 56				
Q71 Comment on Paragraph 57				
176. Global Federation of Insurance Association	Global	No	GFIA notes that this competition for a limited talent pool is a strain on resources of human capital for all parties.	-Noted and see revisions at paragraphs 58 and 59 of the Issues Paper
177. General Insurance Association of Japan	Japan	No	We recognize that this section, Resourcing cyber expertise, is a statement of the difficulty that regulators are having in securing professionally skilled (human) resources. As the demand for specialized skilled resources exceeds the supply for shared resources, both regulators and the industry are focusing their efforts on securing such resources. While we do not object to the Carnegie Endowment for International Peace´s view described in Paragraph 57, we propose deleting the IAIS's interpretation: This means that supervisory authorities and insurers are competing for skilled staff and intensifying the difficulty for authorities to attract and retain specialists, as it could mislead interested parties into believing that industry initiatives are causing the resource shortage problem. Or, it should be stated that there are significant shortages in all sectors, and that it is difficult for supervisory authorities and insurers alike to secure appropriate human resources.	-See revisions at paragraphs 58 of the Issues Paper
Q72 Comment on Paragraph 58				
180. National Association of Insurance	USA, NAIC	No	Recommend the following edit to avoid using duplicating word choice: "One consequence of skills shortages is that the advancement of supervisory	-See revisions at paragraph 59 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Commissioners (NAIC)			frameworks over cyber resilience may lag behind the growing sophistication of cyber-attacks."	
Q73 General Comments on Section 3.3.1 Lessons learnt from the pandemic				
Q74 Comment on Paragraph 59				
182. General Insurance Association of Japan	Japan	No	With use of the cloud and the increase in remote working facilitated by the pandemic, the system environment is diversifying, and remote access is also advancing with respect to the development environment. Under these circumstances, although the situation may differ among individual insurers, it is necessary to consider cases in which the development environment has a different level of security measures than the production environment (e.g., prioritizing the convenience of development speed based on the characteristics of retained data). In addition, we would like to receive information on trends in technical countermeasures, as well as guidelines on countermeasures that are positioned as important to respond to the latest threat trends, so that insurers can utilize them as a reference when making investment plans to strengthen security measures.	-Noted
Q75 General Comments on Section 3.3.2 Supervisory approaches				
184. Global Federation of Insurance Association	Global	No	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.	-Noted and see response to comments 57 and 110 on proportionality and confidentiality
Q76 Comment on Paragraph 60				
186. Global Federation of Insurance Association	Global	No	GFIA supports the continued use of tabletop exercises.	-Noted
187. General Insurance Association of Japan	Japan	No	We would like to receive information on useful best practices in each country, as appropriate, through various research reports by external experts and constructive dialogues with supervisory authorities.	-Noted

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
189. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	First sentence of the "Tabletop Exercises" example: "Working with US state and federal supervisors, law enforcement agencies, and other officials, under the auspices of the Treasury Department's "Hamilton" programme, the National Association of Insurance Commissioners (NAIC) facilitates tabletop exercises with insurers and supervisors to explore cyber incident response and recovery." For consistency of the British English spelling used throughout the document, consider changing "programs" to "programmes" in the second sentence under Tabletop Exercises. "This aims to enhance cyber response programmes of insurers and supervisors by discussing key methods supporting pre-emptive and/or reactive responses to potential threats."	-Agreed
Q77 Comment on Paragraph 61				
190. Insurance Europe	Belgium	No	The first bullet point introduces the possibility of self-assessment questionnaires, which Insurance Europe does not consider to be appropriate tests.	-Noted
191. Global Federation of Insurance Association	Global	No	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.	-Noted
192. General Insurance Association of Japan	Japan	No	In the second bullet point, vulnerability assessments include platform assessments, web application assessments, and smartphone application assessments. Given that each has a different diagnostic target, we believe it would be acceptable to describe them at the overview level. In addition, there are also cloud-based vulnerability assessments, which can be performed by a third party or in-house using tools such as CSPM to check security settings in the cloud. Since this IP also describes the increase in cyber risk due to the use of cloud computing, it would be acceptable to mention it in one of the sections. Regarding "reporting of micro-level data to a supervisory authority" in the third bullet	-Noted -IAIS guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory material

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			point, reporting in a uniform format will help to get a complete picture of the threat. In the fifth and sixth bullet points, we understand that instead of uniformly requiring insurers to conduct Red Team Tests, it is recommended that supervisors establish criteria based on the characteristics of the system and combine it with "Scenario-Based Tests", and that it is acceptable for insurers to decide whether or not to conduct such testing.	
195. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	The first bullet point requires two corrections, as follows: "Self-assessment Questionnaires - involves entities performing self-assessments of the quality of their cyber resilience framework, the responses to which provide a snapshot of the entities' cyber resilience capabilities and vulnerabilities." Suggest the Vulnerability Assessments bullet point be expanded to indicate that these tools are automated scans that check for exploitable known vulnerabilities and culminate in a report on risk exposure. Suggest changing "Cyber incident reporting" to "Cyber Incident Reporting" for case consistency with other titles throughout the document. Suggest changing "Scenario-Based Testing" to "Scenario-based Testing", for case consistency with other hyphenated titles throughout the document.	-See revisions at paragraph 62 of the Issues Paper
Q78 Comment on Section 3.4 IT third-party outsourcing				
197. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest additional clarification in this section regarding what is considered a critical and important IT service. As mentioned in paragraph 68, third-party provider risk goes beyond just those that provide IT services.	-The Issues Paper does not attempt to define critical and important IT services -See also revisions at paragraphs 63-65 of the Issues Paper
Q79 Comment on Paragraph 62				
198. Insurance Europe	Belgium	No	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	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
199. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
200. General Insurance Association of Japan	Japan	No	We would appreciate clarification of the "important IT services" and "concentration risks" definition. Given the number of third-party service providers, an insurer's practice may be to concentrate on certain third-party service providers. A uniform avoidance of concentration could undermine the efficiency of insurers. (Notes) Concentration risk is described in Paragraph 63, but we believe there is still room for clarification on the following points: - What is considered to be "concentration" and to what degree of concentration (e.g., at least for sales and profits, if the business requires resiliency due to social demands, we believe that the company will have no choice but to take extensive	-See response to comment 197

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			measures, including use of a backup plan.). - What kind of outsourced operations are covered? - What will be done in the event of a vendor lock-in or other situations where no alternative is available?	
202. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	The last sentence ends awkwardly with two terms that mean essentially the same thing. Recommend striking some text to remove the redundancy. Additionally, "third party" should be hyphenated because it is used as an adjective rather than a noun. "However, an area where both supervisory requirements and financial institutions' risk management processes remain less advanced is the identification and management of concentration risks associated with the provision of critical IT services to firms by third-party service providers."	-See revisions at paragraph 63 of the Issues Paper
Q80 Comment on Paragraph 63				
203. General Insurance Association of Japan	Japan	No	We would appreciate clarification of the "concentration risks" definition. Given the number of third-party service providers, an insurer's practice may be to concentrate on certain third-party service providers. Avoiding uniform concentration could undermine the efficiency of insurers.	-The IAIS is engaged in cross-sector work on regulatory and supervisory issues related to outsourcing and third-party relationships -See also revisions at paragraph 63-64 of the Issues Paper
Q81 Comment on Paragraph 64				
205. Global Federation of Insurance Association	Global	No	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.	-Noted
206. General Insurance Association of Japan	Japan	No	When discussing the supervisory framework and practices, coordination with geopolitical risk initiatives should also be considered.	-Noted

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Q82 Comment on Paragraph 65				
208. Global Federation of Insurance Association	Global	No	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.	-Noted
209. General Insurance Association of Japan	Japan	No	In addition to coordination between the insurance industry and supervisory authorities in several countries and third-party service providers, coordination with governments and other industries may also be necessary. Furthermore, geopolitical risks need to be considered in the tense international situation.	-Noted
Q83 Comment on Paragraph 66				
Q84 Comment on Paragraph 67				
212. General Insurance Association of Japan	Japan	No	We note that "…as concentration risks frequently arise from a lack of competition and substitutability in the market, insurers may have limited capability to address the nature of this risk in isolation". There are cases where a financial institution requires a high level of response from an outsourcing company, but the company is unable or unwilling to meet the request. As such, it is considered that establishing "minimum required measure standards when undertaking certain tasks for a financial institution", for example, at the national or industry level would help raise the level of outsourced services. It is necessary to consider working with the non-insurance financial sector to encourage the development of regulations for third-party service providers, taking into account the benefits of using third-party services.	-Noted and the IAIS thanks respondents for their suggestions for potential future work -
Q85 Comment on Paragraph 68				
214. General Insurance	Japan	No	We would appreciate clarification of the "concentration risks" definition.	-See response to comment 203

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Association of Japan			Given the number of third-party service providers, an insurer´s practice may be to concentrate on certain third-party service providers. Avoiding uniform concentration could undermine the efficiency of insurers.	
216. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest the following edits: "Other examples of third-party services often used by insurers that may present concentration risks include processes for annuities, payroll and benefits administration, investment management, claims processing and resolving customer queries."	-See revisions at paragraph 69 of the Issues Paper
Q86 Comment on Section 3.4.1 Lessons learned from the pandemic				
Q87 Comment on Paragraph 69				
Q88 Comment on Paragraph 70				
Q89 Comment on Paragraph 71				
221. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	The contractual relationship is not at issue, so suggest identifying the third parties as simply providers: "This was associated with entities having in place numerous arrangements in the same geographic area, resulting in a dependence on one or a few providers in that area for the delivery of services."	-See revisions at paragraph 72 of the Issues Paper
Q90 Comment on Section 3.4.2 Supervisory approaches				
222. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work -See also the responses to comments 57 and 110 on proportionality and confidentiality

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
223. General Insurance Association of Japan	Japan	No	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 coordinating with other areas of the financial sector, governments, and other industries to encourage development of third-party service provider regulations, while taking into account the benefits of using such third-party services. In addition, as described in Paragraph 73, it is impossible for a particular insurer to know which third-party service provider is being used by other players in the industry, nor for what systems and processes. In such a situation, we believe that it may distort the competitive environment if the supervisory authority instructs or recommends, for example, "Consider using another vendor in conjunction with this cloud provider's service due to aggregation risk".	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q91 Comment on Paragraph 72				
225. Global Federation of Insurance Association	Global	No	This must take into consideration the impact on insurers from an operational perspective.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
226. General Insurance Association of Japan	Japan	No	We would appreciate clarification of the "concentration risks" definition. Given the number of third-party service providers, an insurer's practice may be to concentrate on certain third-party service providers. Avoiding uniform concentration could undermine the efficiency of insurers.	-See response to comment 203
Q92 Comment on Paragraph 73				
Q93 Comment on Paragraph 74				
229. Insurance Europe	Belgium	No	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 will, therefore, not have a market-wide view of the industry's reliance on third parties. Supervisory authorities may, therefore, wish to	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
230. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
231. General Insurance Association of Japan	Japan	No	As for "the supervisory authority's ability to directly monitor and manage the resilience of services provided to insurers is further limited" could be read as stating that the supervisory authority's ability to exercise influence is more limited. However, as mentioned several times in Sub-Section 3.4, certain insurers are not in a position to influence IT third-party service providers, especially cloud providers, on their own due to circumstances such as the provider having more bargaining power or being located in a different jurisdiction than the user company. Therefore, we propose the following revision: "…the supervisory authority's ability to directly monitor and manage the resilience of services provided to insurers is limited as well.".	-See revisions at paragraph 75 of the Issues Paper
Q94 Comment on Paragraph 75				
233. Insurance Europe	Belgium	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work. -As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory materials
234. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work. -As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
				on how supervisors should implement supervisory materials
Q95 Comment on Paragraph 76				
236. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work. -As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory materials
237. General Insurance Association of Japan	Japan	No	Consistency of reporting definitions and requirements is important. If there is any information, such as drafts under consideration or prior cases, that may be helpful to keep in mind and utilize in response, we would appreciate early and active sharing.	-Noted and the IAIS thanks respondents for their suggestions for potential future work. -As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory materials
Q96 Comment on Paragraph 77				
239. Institute of International Finance	Global	No	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.	-See response at comment 3

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
240. General Insurance Association of Japan	Japan	No	The adoption of the multi-cloud / multi-vendor approach and exit / portability strategies should be carefully considered, including the unique characteristics of the insurance industry and cost effectiveness.	-See response at comment 3
Q97 General Comments on Section 3.5 Business continuity management				
242. Institute of International Finance	Global	No	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 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.	-Noted
243. General Insurance Association of Japan	Japan	No	Next-generation BCPs may focus on the resources (e.g., human, equipment/facilities, and IT) that can be damaged. In a resource-based BCP, general responses can be taken for each damaged resource, regardless of the incident, and resilient responses can be expected. In order to promote BCM, it is crucial to clarify the contents of important operations that must be maintained and continued in the event of a disaster, and the resources required to maintain and continue these operations. Resources should not be limited to human resources and commodities (including systems), but should also include	-Noted - the IAIS thanks respondents for their suggestions for potential future work and see also text at section 3.5.2 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			the business continuity of outsourcing partners, which should be considered without omission. Expanding the scope of BCM to a wide range of incidents and operations may result in the dispersion of resources, and lower prioritization of response matters. Therefore, it is necessary to first consider the impact of an incident on operations within the framework of BCM. It is considered more effective to apply the existing BCP mutatis mutandis, and if the scope of BCM is to be expanded, the difficulty of feasibility should also be taken into consideration.	
Q98 Comment on Paragraph 78				
246. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest using a different word for the following sentence, as to not limit it to only speed: "An operational disruption, degradation or interruption in the activities of an insurer or any of its service providers could jeopardise its ability to meet its commitments to its insureds and other partners."	-See revisions at paragraph 79 of the Issues Paper
Q99 Comment on Paragraph 79				
Q100 Comment on Paragraph 80				
249. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Second sentence, similar to the first comments and comments for paragraph 35, recommend adding some additional context around "BCP" or at least referencing an earlier explanation.	-See revisions at paragraph 17 of the Issues Paper
Q101 Comment on Paragraph 81				
Q102 Comment on Paragraph 82				
253. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Second sentence, since the IAIS may follow up on some of these considerations, suggest noting that here: "The following aspects of BCM are identified as challenges that could benefit from further analysis by the IAIS and/or cooperation amongst supervisory authorities:"	-See revisions at paragraph 83 of the Issues Paper
Q103 Comment on Paragraph 83				

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
254. General Insurance Association of Japan	Japan	No	It is stated that "consider BCM in the context of their critical operations and all key internal/external dependencies (including third parties' BCPs)". We would appreciate clarification on the specifics and effectiveness of this.	-See revisions at paragraph 84 of the Issues Paper
Q104 Comment on Paragraph 84				
257. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Suggest adding the parenthetical reference "(BIA)" following "Business Impact Analysis." Also, suggest the following addition to include an example of another area that could be contemplated in a BCP. "For example, the need to consider availability in BCPs could be extended to consider the consequences of loss of confidentiality and integrity of information for important business services when business impact analysis (BIA) and risk assessment are performed (information security / cyber preparedness could be integrated into broader BCP and enterprise risk management [ERM]), or how the insurer would handle the loss of a significant number of employees."	-See revisions at paragraph 85 of the Issues Paper
Q105 Comment on Paragraph 85				
259. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	If the BIA parenthetical reference is added to paragraph 84, then suggest changing the last sentence accordingly. Additionally, the last sentence of the paragraph should be singular. "Continuity assumptions that proved inadequate during the pandemic have led to a review of the criticality of some existing processes and the adoption of different time frames (eg immediate, short, medium and long term) in many operational continuity strategies, depending on the results of their BIA and the needs and resources of each insurer."	-See revisions at paragraph 86 of the Issues Paper
Q106 Comment on Paragraph 86				
261. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	First and second sentences, recommend the following edits. We can already observe that remote work is more permanent. Also, it should be clarified that any additional expenses for remote work are likely attributed to IT security, as remote work in general is often cheaper for organizations.	-See revisions at paragraph 87 of the Issues Paper

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			"Although hybrid work arrangements have become more permanent features, in practice remote working policies may vary significantly. Some institutions may consider arrangements that limit the amount of time staff can work from home to avoid additional expenses on IT security."	
Q107 Comment on Paragraph 87				
262. General Insurance Association of Japan	Japan	No	We would like to request that the supervisory authorities provide us with their findings as appropriate, as they will contribute to BCM considerations at each insurer.	-Noted
Q108 General Comments on Section 3.5.1 Lessons learnt from the pandemic				
Q109 Comment on Paragraph 88				
266. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Recommend replacing "cyberattacks" with "cyber-attacks" in the last bullet point for consistency with the other eight occurrences of this word throughout the document. "It was often seen that third parties had the capability of offering technology solutions that are more secure, resilient, and flexible than financial institutions' own existing technology solutions, which sometimes rely on legacy systems." The third bullet point is cumbersome but can possibly be repaired by striking one word. "Growing customer expectations in relation to the time to recovery and level of recovery, and in terms of effective communication from insurers - ie when a disruption occurs, progress in recovering, mitigation measures to ensure they can still get serviced, and notification of when services are restored;"	-Agreed
Q110 Comment on Paragraph 89				
Q111 General Comments on Section 3.5.2 Supervisory approaches				
268. Global Federation of Insurance Association	Global	No	GFIA recommends that supervisory approaches generally be cognizant 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	-Noted

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			conflicting requirements or laws. GFIA encourages alignment with ongoing domestic initiatives.	
Q112 Comment on Paragraph 90				
270. Insurance Europe	Belgium	No	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.	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory materials
271. Global Federation of Insurance Association	Global	No	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.	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory materials
272. General Insurance Association of Japan	Japan	No	Since BCM and operational resilience differ from one insurer to another, we would like to confirm that various measures are to be taken at the discretion of insurers based on the actual situation. It should also be noted that in addition to changes in the work environment of insurers, society as a whole is shifting to a hybrid work environment, which is changing the products and services offered by insurers, as well as the business model itself. Indeed, the entire business is undergoing a transformation.	-As noted on the IAIS website, guidance materials do not create requirements, and Issues Papers are primarily descriptive and are not meant to create expectations on how supervisors should implement supervisory materials
Q113 General Comments on Section 4 Summary of observations and potential future areas of IAIS focus				
274. Insurance Europe	Belgium	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
275. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q114 Comment on Paragraph 91				
Q115 Comment on Paragraph 92				
278. Insurance Europe	Belgium	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
279. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work -The text quoted in the Comment (from Paragraph 93 of the draft Issues Paper) is an observation and not a statement of intention.

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
280. General Insurance Association of Japan	Japan	No	Even if existing mechanisms for information sharing are used, consideration should be given to limit the scope to truly necessary information and to avoid excessive burdens on insurers. We believe that information sharing should be conducted carefully, with sufficient consideration given to the necessity of information sharing, and appropriate safeguards applied.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q116 Comment on Paragraph 93				
282. Global Federation of Insurance Association	Global	No	We agree and support the need for harmonisation.	-Noted
283. General Insurance Association of Japan	Japan	No	Given that the changing environment and associated risks require swift and proper responses, spending too much time on efforts to harmonize definitions and terminology is undesirable and may lead to rigid interpretations. As a result, we believe this could become an obstacle to swift responses. Rather, we believe that it would be more beneficial from the perspective of swift and proper responses to align insurers, supervisors, and the insurance sector as a whole in recognizing the necessity and significance of enhancing operational resilience. Therefore, we propose that Paragraph 93 be revised as follows: In order to promote information sharing among insurers, supervisory authorities, and more broadly across the whole insurance sector, it would be beneficial to align perceptions on the need for and significance of enhancing operational resilience.	-Noted
Q117 Comment on Paragraph 94				
Q118 Comment on Paragraph 95				
287. General Insurance Association of Japan	Japan	No	Although insurer approaches to escalating cyber incidents to supervisory authorities will be informed by the work of the FSB, it should be flexible enough to accommodate the circumstances of the insurance sector in each country.	-Noted
Q119 Comment on Paragraph 96				

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
289. Insurance Europe	Belgium	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
290. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
291. General Insurance Association of Japan	Japan	No	We believe that a multi-vendor strategy should take into account the possibility of higher cost burdens, not only for small and medium-sized entities, but also for large insurers. In order to contribute to each insurer's future policy discussions, we would appreciate information on supervisory practices and methodologies, as appropriate.	-See revisions at paragraph 78 and 97 of the Issues Paper
293. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	Revision to the first sentence to address a typo: "Based on the observations outlined in section 3.4 4, areas that may benefit from further consideration include:" In the fourth bullet point, the last sentence identifies small and medium-sized entities but neither qualifies nor quantifies those terms. Accordingly, recommend modifying as follows to denote all but the largest insurers: "However, it is recognised that these are complex and costly tools, in particular for smaller entities."	-See revisions at paragraph 97 of the Issues Paper
Q120 Comment on Paragraph 97				
Q121 Comment on Paragraph 98				

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
296. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	First bullet, suggest edit to reflect that the sector is already integrating BCM into other risk management functions: "How the sector is approaching evolutions in BCM best practices, in particular in relation to the need to continue to integrate BCM with other relevant risk management functions to remove silos and ensure that BCM frameworks consider the implications of disruptions stemming from cyber and IT third-party outsourcing risks;"	-See revisions at paragraph 99 of the Issues Paper
Q122 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.				
297. Insurance Europe	Belgium	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
298. Global Federation of Insurance Association	Global	No	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	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			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.	
299. Institute of International Finance	Global	No	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 while recognizing, as noted above, that certain terminology used in the banking sector is not appropriate for the insurance sector.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
300. General Insurance Association of Japan	Japan	No	While all of the stated descriptions are important, the situation in each country differs (e.g., there are regional differences in the degree of dependence on IT outsourcing (generally active in Europe and the US)). Therefore, it is not appropriate to set priorities, but rather to consider them concurrently, taking into account their interconnectedness. When prioritizing, please make sure that there is consensus among the parties concerned based on the impact on the project and its usefulness, and that it is acceptable.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
301. The Life Insurance Association of Japan	Japan	No	While four observations are all important, we believe that "information sharing" has the highest priority. Enhanced, prompt and accurate information sharing on cyber incidents and exchange of views on changing circumstances will help improve the measures to address risks related to "cyber resilience," "IT third-party outsourcing" and "BCM".	-Noted and the IAIS thanks respondents for their suggestions for potential future work
303. DGSFP	Spain	No	All the four points (Information sharing, Cyber resilience, IT third-party outsourcing, Business continuity management) are essential and interconnected. Cyber resilience can be a priority since it is complex and maybe less developed than the other topics. Also information sharing can be a priority, but bearing in mind that it is a very sensitive issue.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
304. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	In our view, cyber incident reporting and concentration risk (as outlined under "IT third-party outsourcing) are key areas that could benefit from additional IAIS discussion. These are areas require supervisory coordination on jurisdictional and global levels and also have implications beyond the insurance sector.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q123 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?				
305. Insurance Europe	Belgium	No	Insurance Europe fully agrees with the need for a greater convergence in cyber resilience framework.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
306. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
307. Institute of International Finance	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
308. The Geneva Association	International	No	Whilst the IAIS discusses the challenges that supervisory authorities may face in overseeing the services that third parties provide to the regulated firms (where such third parties remain outside the regulatory perimeter), the scope of regulated firms' oversight, as 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 the international level (potentially building on 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 and reduce the gaps in oversight which could result from a less uncoordinated approach. 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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
309. General Insurance Association of Japan	Japan	No	Geopolitical risks, such as Russia´s recent invasion of Ukraine, could affect operations. It should be noted that geopolitical risks are not limited to the insurance sector and must be addressed in cooperation with a wide range of industries, and that such situations change on a daily basis.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
310. The Life Insurance	Japan	No	Currently, we do not believe there are any other additional issues to be addressed besides those identified in this Issues Paper.	-Noted

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
Association of Japan				
313. DGSFP	Spain	No	No. The document is very comprehensive and includes all relevant aspects identified so far,	-Noted
314. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	If the third-party provider management discussed in this Issues Paper is strictly related to IT services, additional discussion on third-party vendor management as a whole could be useful. If, for instance, a company's producer suffers a cyber-attack or data breach or isn't able to resume business in a timely manner after a disaster, that impacts the company's operations, as well. Also, as touched on in Annex 1, there is very little consideration that has been given to fourth-party risks to date. Another item that was touched on briefly but wasn't mentioned as a potential future area of focus is the need to be able to attract and retain talent with expertise in cybersecurity. Training existing staff is a good response, but there has to be existing staff that is interested and there has to be someone or some way to train them. After the training, there still needs to be a way to retain them. Cybersecurity experts are at a premium and although large insurers have the money to pay them, small and mid-sized companies and regulatory agencies don't have the budget.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
Q124 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?				
315. Insurance Europe	Belgium	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
316. Global Federation of Insurance Association	Global	No	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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
317. Institute of International Finance	Global	No	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.	n-Noted and the IAIS thanks respondents for their suggestions for potential future work
318. The Geneva Association	International	No	Information exchange is essential for the effective oversight of firms' operational resilience which is often tied with the third parties that operate internationally. In this context, 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, 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.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
319. General Insurance Association of Japan	Japan	No	Information sharing and dialogue on best practices led by the IAIS would help to strengthen the resilience of the whole insurance sector. However, since it is assumed that there will be cases where responses will differ depending on the customs and culture of each country, it would be appropriate to share, as a reference, when examining the operations of each country, industry, and insurer. When collecting information, we request that consideration be given to limiting the	-Noted and the IAIS thanks respondents for their suggestions for potential future work

Organisation	Jurisdiction	Confidential	Answer	IAIS Response
			data to what is truly necessary so as not to impose an excessive burden on insurers. In addition, the necessity of information sharing among supervisory authorities should be fully considered, and information should be shared carefully, with appropriate safeguards applied.	
320. The Life Insurance Association of Japan	Japan	No	We find value in the IAIS facilitating cross-border information sharing and are willing to participate. However, we would like to ask the IAIS to give due consideration as not to cause excessive burden on insurers participating in the above information sharing.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
323. DGSFP	Spain	No	We consider that it is an important aspect that have to be discussed internationally and the role of IAIS is crucial in this respect, in particular to identify the potential differences between the different frameworks. In any case confidentiality issues have to be an essential part of the analysis.	-Noted and the IAIS thanks respondents for their suggestions for potential future work
325. National Association of Insurance Commissioners (NAIC)	USA, NAIC	No	We think there is value in this assuming it is folded into an existing IAIS forum, such as the revamped Supervisory Forum. It might also be required for such information sharing that participants are signatories to the MMoU. Depending on the forum, we might be interested in participating.	-Noted and the IAIS thanks respondents for their suggestions for potential future work