Questions	Comments
General Comments	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.
Para 5	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”.
Para 34	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.
Para 37	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.
Para 38	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.
Para 40	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.

Para 42	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.
Para 43	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.
Para 44	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:
Para 47	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.
Para 48	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.
Para 49	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.
Para 53	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.
Para 54	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.
Para 55	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.
Para 57	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.
Para 59	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.
Para 60	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.
Para 61	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 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.
Para 62	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 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?
Para 63	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.
Para 64	When discussing the supervisory framework and practices, coordination with geopolitical risk initiatives should also be considered.
Para 65	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.
Para 67	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.
Para 68	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.

Section 3.4.2	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”.
Para 72	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.
Para 74	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.”.
Para 76	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.
Para 77	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.
Section 3.5	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 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.
Para 83	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.
Para 87	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.
Para 90	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.
Para 92	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.
Para 93	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.
Para 95	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.
Para 96	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.
Question 1	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.
Question 2	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.
Question 3	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 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.